09/404,547

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　７月２３日

出願番号
Application Number: 平成１１年特許願第２０９８３６号

出願人
Applicant (s): 株式会社東芝

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年１０月　８日

特許庁長官
Commissioner,
Patent Office

近藤隆

【書類名】　特許願

【整理番号】　A009903887

【提出日】　平成11年 7月23日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 12/00

【発明の名称】　中継装置及び通信装置

【請求項の数】　17

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　斉藤　健

【発明者】

【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

【氏名】　高畠　由彰

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【先の出願に基づく優先権主張】

【出願番号】　平成10年特許願第292824号

【出願日】　平成10年 9月30日

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705037

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　中継装置及び通信装置

【特許請求の範囲】

【請求項１】

第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

前記第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして前記第１のネットワーク側に開示する代理構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記第１のネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を前記第２のネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、

前記第１のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、

このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記第２のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段とを具備したことを特徴とする中継装置。

【請求項２】

第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

第１及び第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、

前記第１又は第２のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、

このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段と、

前記第１又は第２のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛であり、前記コンテンツ保護情報から得られるコンテンツ鍵で保護されたコンテンツを受信するコンテンツ受信手段と、

このコンテンツ受信手段で受信した前記コンテンツに変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ転送手段とを具備したことを特徴とする中継装置。

【請求項３】

前記コンテンツ保護情報は、前記第１のネットワーク上の装置又はサービス又はサブユニットと、前記第２のネットワーク上の装置又はサービス又はサブユニット間の認証及び又は鍵交換を含むコンテンツ保護の手続きに関する情報であることを特徴とする請求項２に記載の中継装置。

【請求項４】

第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

第１及び第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、

前記第１のネットワーク上の装置又はサービス又はサブユニットと、自中継装

置の間で、コンテンツ保護の手続きを行う第１のコンテンツ保護手段と、

前記第２のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第２のコンテンツ保護手段と、

前記第１又は第２のいずれか一方のネットワーク上の装置から、前記代理構成手段で開示した自中継装置上の装置又はサービス又はサブユニット宛であり、前記第１又は第２のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、

前記コンテンツ受信手段で受信したコンテンツを、前記第１又は第２のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第１又は第２のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備したことを特徴とする中継装置。

【請求項５】

前記第１のコンテンツ保護手段と、前記第２のコンテンツ保護手段で用いられる暗号化方式は異なる方式であるか、又は異なる鍵情報に基づくものであることを特徴とする請求項４に記載の中継装置。

【請求項６】

前記コンテンツ受信手段と、前記コンテンツ送信手段は同一のＬＳＩに封止されていることを特徴とする請求項４に記載の中継装置。

【請求項７】

前記第１のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第１の鍵情報と、前記第２のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第２の鍵情報とを同一のものとすることを特徴とする請求項４に記載の中継装置。

【請求項８】

前記第１又は第２のいずれか他方のコンテンツ保護手段における前記コンテンツ保護の手続きは、所定の鍵情報を用いて、コンテンツ単位又はサービス単位又はサブユニット単位で行なうことを特徴とする請求項７に記載の中継装置。

【請求項９】

前記第１及び第２のネットワーク上の装置又はサービス又はサブユニットから

、該装置の認証フォーマットの有無を含む構成情報を受信する構成情報受信手段と、

前記構成情報受信手段で受信した各構成情報に基づいて、該装置又はサービス又はサブユニットの構成認識を行う構成認識手段とを更に具備したことを特徴とする請求項２または４に記載の中継装置。

【請求項１０】

第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

前記第１のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第１のコンテンツ保護手段と、

前記第２のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第２のコンテンツ保護手段と、

前記第１又は第２のいずれか一方のネットワーク上の装置から、自中継装置上の装置又はサービス又はサブユニット宛であり、前記第１又は第２のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、

前記コンテンツ受信手段で受信したコンテンツを、前記第１又は第２のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第１又は第２のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備し、

前記第１のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第１の鍵情報と、前記第２のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第２の鍵情報とを同一のものとすることを特徴とする中継装置。

【請求項１１】

ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、

前記ネットワーク上の他の装置に対して、自通信装置のアドレスを付与した暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは更に自通信装置のアドレスおよび該コンテンツを一意に識別可能な識別子を付与して、送信するコンテンツ送信手段と、

前記ネットワーク上の他の装置から、前記仮想チャネル上を介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを受信する受信手段と、

この問合せに応答して、前記ネットワーク上の他の装置に対し、該当するサービスまたはサブユニットまたはプラグについての通知をする通知手段とを具備することを特徴とする通信装置。

【請求項１２】

ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、

前記ネットワーク上の他の装置から、該ネットワーク上の他の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該ネットワーク上の他の装置が該コンテンツを一意に識別可能な識別子が付与された形で、受信するコンテンツ受信手段と、

前記ネットワーク上の他の装置に対して、前記仮想チャネルを介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを送信する送信手段と、

前記ネットワーク上の他の装置から、前記問合せに該当するサービスまたはサブユニットまたはプラグについての通知を受信する受信手段とを具備することを特徴とする通信装置。

【請求項１３】

ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置に対して、暗号化されたコンテンツを、送信アドレス、送信ポート、受信アドレスおよび受信ポートの組みで識別されるフロー

を介して送信または受信するコンテンツ転送手段と、

前記ネットワーク上の他の装置との間で、予め定められた論理ポートを用いて、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段とを具備し、

前記所定のコンテンツ保護手続きを行なう場合には、これを前記フローの単位で行なうことを特徴とする通信装置。

【請求項１４】

前記所定のコンテンツ保護手続きに含まれる少なくとも一部の手続きにおいてやり取りされる情報に前記フローの識別子を付与することを特徴とする請求項２１に記載の通信装置。

【請求項１５】

ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、

前記ネットワーク上の他の装置に対して、送信側の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該送信側の装置が該コンテンツを一意に識別可能な識別子を付与された形で、送信または受信するコンテンツ送受信手段とを具備し、

前記所定のコンテンツ保護手続きに含まれる少なくとも一部の手続きにおいてやり取りされる情報に、前記暗号化されたコンテンツのやり取りを行うサービス、サブユニット、仮想チャネルもしくはプラグの識別子、または前記送信側の装置が前記コンテンツを一意に識別可能な識別子のうちの少なくとも一つを付与することを特徴とする通信装置。

【請求項１６】

第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

第１のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き行う

第１のコピープロテクション処理手段と、

第２のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き第２のコピープロテクション処理手段と、

前記第１のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、

前記第１のインタフェース手段から受信された前記暗号化されたデータを、前記第１のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、

前記復号化されたデータを、別の符号化形式のデータに変換する変換手段と、

前記復号化されたデータを、前記第２のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、

前記暗号化されたデータを、前記第２のインタフェース手段へ転送するコンテンツ送信手段とを具備したことを特徴とする中継装置。

【請求項１７】

前記第２のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第１のネットワーク側に開示するとともに、前記第１のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第２のネットワーク上の装置またはサービスまたはサブユニット宛に送信するとともに、

前記第１のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第２のネットワーク側に開示するとともに、前記第２のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第１のネットワーク上の装置またはサービスまたはサブユニット宛に送信する代理構成手段を更に具備し、

前記代理構成手段は、前記第１または第２の一方のネットワーク上の装置と、前記第１または第２の他方のネットワーク上の装置またはサービスまたはサブユ

ニットとの、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第１または第２の一方のコピープロテクション処理手段を用いて前記一方のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記第１または第２の他方のコピープロテクション処理手段を用いて前記他方のネットワーク上の装置またはサービスまたはサブユニットと該所定のコンテンツ保護手続きを行うことを特徴とする請求項２４に記載の中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＩＥＥＥ１３９４バスや無線ネットワーク等のネットワーク間のデータ転送を中継する中継装置及びＩＥＥＥ１３９４バスや無線ネットワーク等のネットワークを介して通信を行う通信装置に関する。

【０００２】

【従来の技術】

近年、デジタル放送の開始や、デジタルＡＶ機器の発売等、いわゆる「家庭ＡＶ環境のデジタル化」が大きな注目を集めている。デジタルＡＶデータは、様々な圧縮が可能、マルチメディアデータとしても処理が可能、何回再生しても劣化がない、等の優れた特徴を持ち、今後その用途はますます広がっていくものと考えられる。

【０００３】

しかしながら、このデジタルＡＶ技術には、反面、「コンテンツの不正コピーが容易に行える」という側面もある。すなわち、どのようなデジタルコンテンツについても、原理的に「ビットのコピー」で、元どおりの品質の、しかも未来永劫にわたって一切劣化のない複製が作れてしまうため、いわゆる「不正コピー」の問題が発生する。

【０００４】

この「不正コピー」を防ぐための技術がいくつか検討されている。その中の一つが、ＣＰＴＷＧ（コピープロテクション技術ワーキンググループ）で検討され

ている「１３９４ＣＰコンテンツ保護システム仕様（１３９４ＣＰ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ）」である。この技術は、ＩＥＥＥ１３９４バスに接続されたノード間で、転送するコンテンツ（例えばＭＰＥＧデータ等）について、送受信ノードの間で予め認証手続きを行い、暗号鍵（コンテンツキー）を共有できるようにしておき、以降は転送するコンテンツを暗号化して転送し、認証手続きを行った両者以外はコンテンツが読めないようにする技術である。このようにすることにより、認証手続きを行っていないノードは、コンテンツキーの値がわからないため、転送されているデータ（暗号化されているデータ）をたとえ取り込むことができたとしても、この暗号を復号化することはできない。このような認証に参加できるノードは、あらかじめ定められた認証機関が許可したノードのみとしておくことで、不正なノードが暗号鍵を入手することを未然に防ぎ、不正コピーを予め防ぐことが可能になる。

【０００５】

【発明が解決しようとする課題】

ＩＥＥＥ１３９４バスは、最低速度でも１００Ｍｂｐｓ、網そのものに自動構成認識機能が備わっている、ＱＯＳ転送機能を持つ等、非常に優れた特徴を持つネットワークシステムであり、それゆえに家庭向けのデジタルＡＶ向けのネットワークとして、デファクトスタンダードの地位を築いている。

【０００６】

しかし、ＩＥＥＥ１３９４は、これら特徴のゆえに、「ＩＥＥＥ１３９４と、他のネットワークを接続するとき」に様々な制約を生んでいる。例えば、無線網や公衆網とＩＥＥＥ１３９４バスを接続する場合は、これらの網が１００Ｍｂｐｓ以上といった高速性を一般には有していないことや、ＩＥＥＥ１３９４の自動構成認識機能をこれらの網へそのまま拡張する、といった方法が簡単にはとれないことから、ＩＥＥＥ１３９４プロトコルをそのまま無線や公衆網に拡張する、といった方法を使うことはできない。そこで、ＩＥＥＥ１３９４と、無線網や公衆網などの他網の間にプロトコル変換ゲートウェイを配置し、相互接続する方法や、片方の網上のサービスをもう片方の網のサービスとして提供するいわゆる代

理サーバの方法等が提案されている。

【０００７】

これらの方法を、従来の技術で述べた１３９４コピープロテクションに適用しようとした場合、現状では該コピープロテクション技術がＩＥＥＥ１３９４バスについてのみ定められている状況である。このコピープロテクション技術を「ＩＥＥＥ１３９４と、他のネットワークを接続するとき」に拡張するための技術はないのが現状である。

【０００８】

本発明は、上記事情を考慮してなされたもので、コピープロテクション技術をＩＥＥＥ１３９４のみならず、これと相互接続された他網にも拡張可能な中継装置及び通信装置を提供することを目的とする。

【０００９】

また、本発明は、同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置及び通信装置を提供することを目的とする。

【００１０】

【課題を解決するための手段】

本発明（請求項１）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、前記第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして前記第１のネットワーク側に開示する代理構成手段と、この装置又はサービス又はサブユニット宛の制御コマンド信号を前記第１のネットワーク側から受信する制御コマンド受信手段と、この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を前記第２のネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、前記第１のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記第２のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段とを具備したことを特徴とする。

【００１１】

本発明（請求項２）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、第１及び第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、前記第１又は第２のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段と、前記第１又は第２のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛であり、前記コンテンツ保護情報から得られるコンテンツ鍵で保護されたコンテンツを受信するコンテンツ受信手段と、このコンテンツ受信手段で受信した前記コンテンツに変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ転送手段とを具備したことを特徴とする。

【００１２】

好ましくは、前記コンテンツ保護情報は、前記第１のネットワーク上の装置又はサービス又はサブユニットと、前記第２のネットワーク上の装置又はサービス又はサブユニット間の認証及び又は鍵交換を含むコンテンツ保護の手続きに関する情報であるようにしてもよい。

【００１３】

本発明によれば、例えば、保護すべきコンテンツの送信もしくは受信を行っているペアである「代理構成手段が提供している第２のネットワーク上の装置またはサービスまたはサブユニット（以下、装置またはサービスまたはサブユニット

を装置等と呼ぶ）」と「第１のネットワーク上の装置」との間において、「第１のネットワーク上の装置」または「代理構成手段が提供している第２のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第１のネットワーク上の装置」または「代理構成手段が提供している第２のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、実際には、中継装置がその手続きを中身を変えることなく中継することによって、そのコンテンツ保護手続きを直接「代理構成手段が提供している第２のネットワーク上の装置等」と「第１のネットワーク上の装置」との間において行うことができる。

【００１４】

また、本発明によれば、保護されるべきコンテンツを、その保護形式を変更することなく受信側に送り届けることができ、コンテンツを保護された形でエンドエンドに送り届けることができる。

【００１５】

本発明（請求項４）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、第１及び第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、前記第１のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第１のコンテンツ保護手段と、前記第２のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第２のコンテンツ保護手段と、前記第１又は第２のいずれか一方のネットワーク上の装置から、前記代理構成手段で開示した自中継装置上の装置又は

サービス又はサブユニット宛であり、前記第１又は第２のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、前記コンテンツ受信手段で受信したコンテンツを、前記第１又は第２のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第１又は第２のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備したことを特徴とする。

【００１６】

本発明によれば、例えば、保護すべきコンテンツの送信もしくは受信を行っているペアである「第２のネットワーク上の装置等」と「第１のネットワーク上の装置」との間において、「第１のネットワーク上の装置」または「第２のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第１のネットワーク上の装置」または「第２のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、例えば、中継装置が、コンテンツ保護手続きをそれぞれ終端することで、結局、「第２のネットワーク上の装置等」と中継装置との間、および中継装置と「第１のネットワーク上の装置」との間で、コンテンツ保護手続きをそれぞれ行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

【００１７】

また、第１のネットワーク上の装置から第２のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、不正コピー等を未然に防ぐことが可能になる。

【００１８】

好ましくは、前記第１のコンテンツ保護手段と、前記第２のコンテンツ保護手段で用いられる暗号化方式は異なる方式であるか、又は異なる鍵情報に基づくものであるようにしてもよい。

【００１９】

好ましくは、前記コンテンツ受信手段と、前記コンテンツ送信手段は同一のＬＳＩに封止されているようにしてもよい。これによって、この復号化手段と暗号

化手段との間は、暗号化されていないコンテンツデータが流れるため、個々にプローブをあてる等して、ここからコンテンツデータを盗聴し、不正コピーを働くことを未然に防止することが可能となる。

【００２０】

好ましくは、前記第１のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第１の鍵情報と、前記第２のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第２の鍵情報とを同一のものとするようにしてもよい。これによって、一方のネットワークから伝えられた、他方のネットワークへ転送された暗号化データの鍵に関する情報（鍵やシード等）を、他方のネットワークへそのまま転送することにより、他方のネットワーク上の装置では該暗号化鍵の再生が可能となるため、コンテンツ受信手段とコンテンツ送信手段との間の暗号復号機能および再暗号化機能が不要となり、中継装置の大幅なコストの低減と、処理速度の高速化を図ることが可能となる。

【００２１】

また、好ましくは、他方のネットワーク側の装置と、暗号化されたデータの転送を行っている場合には、他方のネットワーク上の他の装置からの、暗号化が必要なデータの送信要求は拒否するようにしてもよい。このようにすれば、他方のネットワーク側において、異なる暗号化されたデータ転送を未然に防止することが可能となる。

【００２２】

好ましくは、前記第１又は第２のいずれか他方のコンテンツ保護手段における前記コンテンツ保護の手続きは、所定の鍵情報を用いて、コンテンツ単位又はサービス単位又はサブユニット単位で行なうようにしてもよい。これによって、他方のネットワーク側の装置との間で、複数の暗号鍵を定義できるようになるため、暗号化されたデータを同時に転送することが可能となり、一方のネットワーク上の装置から複数の暗号化データが転送される場合あるいは一方のネットワーク上に複数の装置がある場合等への対処が可能となる。

【００２３】

好ましくは、前記第１及び第２のネットワーク上の装置又はサービス又はサブ

ユニットから、該装置の認証フォーマット（機器証明）の有無を含む構成情報を受信する構成情報受信手段と、前記構成情報受信手段で受信した各構成情報に基づいて、該装置又はサービス又はサブユニットの構成認識を行う構成認識手段とを更に具備するようにしてもよい。これによって、代理構成手段が構成する代理サービスを、自動的に構成することができるようになり、もって、コンテンツ保護手続きに至る手順のプラグアンドプレイでの実現が可能になる。

【００２４】

また、好ましくは、前記代理構成手段は、前記第１のネットワークの装置に対してデータを送信する際に、あらかじめ該第１のネットワークの装置に対して自中継装置が代理構成している該データを送信する装置またはサービスまたはサブユニットを通知するようにしてもよい。これによって、この通知を受信した第１のネットワーク上の装置に対して、どこに認証要求を出せばよいかを通知することが可能になる。

【００２５】

本発明（請求項１０）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、前記第１のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第１のコンテンツ保護手段と、前記第２のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第２のコンテンツ保護手段と、前記第１又は第２のいずれか一方のネットワーク上の装置から、自中継装置上の装置又はサービス又はサブユニット宛であり、前記第１又は第２のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、前記コンテンツ受信手段で受信したコンテンツを、前記第１又は第２のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第１又は第２のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備し、前記第１のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第１の鍵情報と、前記第２のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第２の鍵情報とを同一のもの

とすることを特徴とする。

【００２６】

本発明（請求項１１）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、前記ネットワーク上の他の装置に対して、自通信装置のアドレスを付与した暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは更に自通信装置のアドレスおよび該コンテンツを一意に識別可能な識別子を付与して、送信するコンテンツ送信手段と、前記ネットワーク上の他の装置から、前記仮想チャネル上を介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを受信する受信手段と、

この問合せに応答して、前記ネットワーク上の他の装置に対し、該当するサービスまたはサブユニットまたはプラグについての通知をする通知手段とを具備することを特徴とする。

【００２７】

本発明（請求項１２）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、前記ネットワーク上の他の装置から、該ネットワーク上の他の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該ネットワーク上の他の装置が該コンテンツを一意に識別可能な識別子が付与された形で、受信するコンテンツ受信手段と、前記ネットワーク上の他の装置に対して、前記仮想チャネルを介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを送信する送信手段と、前記ネットワーク上の他の装置から、前記問合せに該当するサービスまたはサブユニットまたはプラグについての通知を受信する受信手段とを具備することを特徴とする。

【００２８】

本発明によれば、特定の仮想チャネルで転送されている暗号化データの送信、あるいは受信それぞれのサブユニットあるいはプラグを特定することが可能となり、以降の認証・鍵交換で、「このサブユニット（あるいはプラグ）から送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

あるいは、本発明によれば、特定の識別子を持って転送されている暗号化データの送信、あるいは受信それぞれのサブユニットあるいはプラグを特定することが可能となり、以降の認証・鍵交換で、「このサブユニット（あるいはプラグ）から送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【００２９】

本発明（請求項１３）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置に対して、暗号化されたコンテンツを、送信アドレス、送信ポート、受信アドレスおよび受信ポートの組みで識別されるフローを介して送信または受信するコンテンツ転送手段と、前記ネットワーク上の他の装置との間で、予め定められた論理ポートを用いて、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段とを具備し、前記所定のコンテンツ保護手続きを行なう場合には、これを前記フローの単位で行なうことを特徴とする。

【００３０】

好ましくは、前記所定のコンテンツ保護手続きに含まれる少なくとも一部の手続きにおいてやり取りされる情報に前記フローの識別子を付与するようにしてもよい。

【００３１】

本発明によれば、フロー毎に異なる鍵の定義ができるようになるため、以降の認証・鍵交換で、「このフローに関する認証・鍵交換を行いたい」と明示するこ

とが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【００３２】

本発明（請求項１５）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、前記ネットワーク上の他の装置に対して、送信側の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該送信側の装置が該コンテンツを一意に識別可能な識別子を付与された形で、送信または受信するコンテンツ送受信手段とを具備し、前記所定のコンテンツ保護手続きに含まれる少なくとも一部の手続きにおいてやり取りされる情報に、前記暗号化されたコンテンツのやり取りを行うサービス、サブユニット、仮想チャネルもしくはプラグの識別子、または前記送信側の装置が前記コンテンツを一意に識別可能な識別子のうちの少なくとも一つを付与することを特徴とする。

【００３３】

本発明によれば、認証・鍵交換で、「このサブユニット、あるいはプラグ、あるいは仮想チャネルから送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

あるいは、本発明によれば、認証・鍵交換で、「このサブユニット、あるいはプラグから、あるいは前記特定の識別子を持って、送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【００３４】

本発明（請求項１６）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェ

ース手段と、第１のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き行う第１のコピープロテクション処理手段と、第２のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き第２のコピープロテクション処理手段と、前記第１のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、前記第１のインタフェース手段から受信された前記暗号化されたデータを、前記第１のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、前記復号化されたデータを、別の符号化形式のデータに変換する変換手段と、前記復号化されたデータを、前記第２のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、前記暗号化されたデータを、前記第２のインタフェース手段へ転送するコンテンツ送信手段とを具備したことを特徴とする。

【００３５】

本発明によれば、第１のネットワークを伝送させるデータが保護されるべきコンテンツであり、且つ、第１のネットワークと第２のネットワークの通信帯域が著しく異なる場合のように、第２のネットワークに元のデータとは異なるデータ形式で転送することが求められた場合に、変換手段によってデータ形式の変換を行いつつ、第１のネットワーク上の装置から第２のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、両区間（両データ形式）においても、不正コピー等を未然に防ぐことが可能になる。

【００３６】

好ましくは、請求項１６に記載の中継装置において、前記第２のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第１のネットワーク側に開示するとともに、前記第１のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第２のネットワーク上の装置またはサービスまたはサブユニット宛に送信するとともに、前

記第１のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第２のネットワーク側に開示するとともに、前記第２のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第１のネットワーク上の装置またはサービスまたはサブユニット宛に送信する代理構成手段を更に具備し、前記代理構成手段は、前記第１または第２の一方のネットワーク上の装置と、前記第１または第２の他方のネットワーク上の装置またはサービスまたはサブユニットとの、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第１または第２の一方のコピープロテクション処理手段を用いて前記一方のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記第１または第２の他方のコピープロテクション処理手段を用いて前記他方のネットワーク上の装置またはサービスまたはサブユニットと該所定のコンテンツ保護手続きを行うようにしてもよい。

【００３７】

本発明によれば、保護すべきコンテンツの送信もしくは受信を行っているペアである「他方のネットワーク上の装置等」と「一方のネットワーク上の装置」との間において、「一方のネットワーク上の装置」または「他方のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「一方のネットワーク上の装置」または「他方のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、実際には、中継装置がそのコンテンツ保護手続きをそれぞれ終端することで、結局、「他方のネットワーク上の装置等」と中継装置、および中継装置と「一方のネットワーク上の装置」との間で、コンテンツ保護手続きを行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

【００３８】

また、好ましくは、請求項１６に記載の中継装置において、前記コンテンツ受信手段は、前記第２のコピープロテクション処理手段を用いて、前記第２のネッ

トワーク上の装置またはサービスまたはサブユニットと、前記所定のコンテンツ保護手続きのうち少なくとも一部を行ってそれが正常に終了した場合に、前記第１のコピープロテクション処理手段を用いて、前記第１のネットワークの装置またはサービスまたはサブユニットと前記所定のコンテンツ保護手続きのうち少なくとも一部を行うようにしてもよい。なお、前記所定のコンテンツ保護手続きのうち少なくとも一部は、例えば、認証手続きである。このようにすれば、第２のネットワーク上の装置またはサービスまたはサブユニットが信頼に足るデバイスであるかどうかを未然に知ることができるようになり、まず第２のネットワーク上の装置等と認証手続きを行い、その後、第１のネットワーク上の装置等との認証に失敗した場合に、第１のネットワーク上の装置等との認証を改めて行わなくてもよい分、通信資源や処理資源の節約になる。

【００３９】

また、本発明に係る通信装置は、第１の装置の制御に供される画面描画のためのプログラムを含む、第１の制御プログラムを受信し、これを稼働するプロセッサ手段と、このプロセッサ手段が描画する画面のうちの少なくとも一部を構成するパネル画面を作成する画面作成手段と、前記パネル画面へのコマンドと、前記第１の装置の制御のためのコマンドとの対応関係を記憶する記憶手段と、前記パネル画面をサブユニットとして第２の装置に公開するサブユニット処理手段と、前記サブユニットへのコマンドを受信した場合、前記記憶手段を参照してこのコマンドを前記第１の装置の制御のためのコマンドに変換して、これを送出する手段とを具備したことを特徴とする。

一般に、前記のような制御プログラムを稼働させるためには、仮想マシンと呼ばれ計算環境を用意する必要があるのに対し、パネル画面を通した機器制御は、簡単なコマンド体型を用意するだけでよいため、簡単な計算環境を用意しておけばよい。本発明によれば、前記制御プログラムを持たない第２の装置に対しても、パネル画面という形で、前記第１の装置の制御インタフェースを提供することが可能になる。

【００４０】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明

は装置に係る発明としても成立する。

【００４１】

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００４２】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【００４３】

（第１の実施形態）

図１は、ある家庭のホームネットワークの全体構成の一例である。

【００４４】

このホームネットワークには、送信ノード１０１、中継ノード１０２、無線ノード１０３の３つが接続されており、送信ノード１０１と中継ノード１０２は（有線の）ＩＥＥＥ１３９４バス１０４に、中継ノード１０２と無線ノード１０３は無線網にそれぞれ接続されている。ただし、後述するような方法で、各々のノードは互いに通信ができるようになっている。

【００４５】

本実施形態では、送信ノード１０１から送出されたＭＰＥＧ映像を、中継ノード１０２で中継し、無線区間を経由して無線ノード１０３に送信する場合を例として説明する。その際に、著作権保護（不正コピーの防止）のために、送信ノード１０１と無線ノード１０３との間で転送されるＭＰＥＧ映像データは暗号化される場合を考える。

【００４６】

なお、図１では、３つのノードを示してあるが、もちろん、これらの他にノードが接続されていてもよい（後述する他の実施形態においても同様である）。

【００４７】

図２に、送信ノード１０１の内部構造の一例を示す。

【００４８】

送信ノード１０１は、内部にＭＰＥＧ映像データを蓄積している装置であり、要求に応じてＭＰＥＧ映像データをＩＥＥＥ１３９４バス１０４を通じて送出する。その際、ＩＥＥＥ１３９４バス上において不法コピーをされることを未然に防止するために、必要な場合には送出するＭＰＥＧ映像データを暗号化して送出する機能を持つ。そのため、ＭＰＥＧ映像データを受信するノードと、認証データ、暗号鍵等の交換を行うための機構も持つ。

【００４９】

図２に示されるように、この送信ノード１０１は、ＩＥＥＥ１３９４インタフェース４０１、ＡＶ／Ｃプロトコルの処理を行うＡＶ／Ｃプロトコル処理部４０２、ＡＶ／Ｃプロトコル内のコピープロテクションに関する処理を行うコピープロテクション処理部４０３、ＩＥＥＥ１３９４を通して送受信されるデータのうち、同期チャネルを通してやり取りされるデータについて送受信するＩＳＯ信号送受信部４０４、ＭＰＥＧ映像のストレージであるＭＰＥＧストレージ部４０６、コピープロテクション処理部４０３から暗号鍵Ｋをもらい、ＭＰＥＧ映像を暗号化してＩＳＯ信号送受信部４０４に送出する暗号化部４０５を有する。ここで、コピープロテクション処理部４０３は、認証のためのフォーマットＡｃｅｒｔを持つ。

【００５０】

次に、図３に、中継ノード１０２の内部構造の一例を示す。

【００５１】

中継ノード１０２は、ＩＥＥＥ１３９４バス側から受信したデータ（ＭＰＥＧ映像データ）を無線区間側にフォワードする機能の他に、ＩＥＥＥ１３９４バス側のノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対してＩＥＥＥ１３９４バス側のノード（本実施形態では送信ノード１０１）の代理サーバとなり、ＩＥＥＥ１３９４バス側のノードの機能を代理で提供する機能が存在する。

【００５２】

図３に示されるように、この中継ノード１０２は、ＩＥＥＥ１３９４インタフェース２０１、無線インタフェース２０２、ＡＶ／Ｃプロトコル処理部２０３、ＩＳＯ信号送受信部２０４、無線区間側の同期チャネルの信号の送受信を行う無線ＩＳＯ信号送受信部２０５、ＩＥＥＥ１３９４バス上のノードの構成情報を収集したり、自らの構成情報（自分がどのような機能を持っているかについての情報等）をＩＥＥＥ１３９４上に広告する機能を持つ１３９４バス構成認識部２０６、ＩＥＥＥ１３９４バス側に対して無線区間側のノードやサービス（サブユニット）を代理で公開したり、無線区間側のノードやサービスへのコマンド等を代理で受け付け、これを無線区間側に必要に応じてプロトコル変換をして送出したり、あるいは無線区間側に対してＩＥＥＥ１３９４側のノード／サービス（サブユニット）の代理公開やコマンドの代理受付／翻訳等を行う代理サブユニット構成部２０７、無線区間上のノードの構成情報を収集したり、自らの構成情報（自分がどのような機能を持っているかについての情報等）を無線区間上に広告する機能を持つ無線区間構成認識部２０９、コピープロテクションに関する処理を行い、１３９４バスと無線区間をまたがるコピープロテクション処理に関しては、やり取りされる情報を透過的にフォワードさせるコピープロテクション制御／フォワード部２１０、無線区間でやり取りされる制御パケットの送受信を行う無線ノード制御パケット送受信部２１１を有する。

【００５３】

次に、図４に、無線ノード１０３の内部構造の一例を示す。

【００５４】

無線区間においていわゆるＩＥＥＥ１３９４プロトコル（物理レイヤプロトコル、リンクレイヤプロトコル等）が稼働している必要は必ずしもなく、ＩＥＥＥ８０２．１１や無線ＬＡＮ等、任意の無線プロトコルを利用することを想定するが、本実施形態では、特に、いわゆるＱＯＳ機能（同期通信機能）を持つ無線網であることを仮定する。ただし、本実施形態は、無線区間部分にＱＯＳ機能が求められると制限されるものではない。

【００５５】

いわゆるＩＥＥＥ１３９４ノードではない無線ノード１０３が、ＩＥＥＥ１３

９４バスにつながれたノード（本実施形態では送信ノード１０１）と通信を行うために、前述のように、中継ノード１０２がＩＥＥＥ１３９４バス上のノードや機能（サブユニット）をエミュレートしている。すなわち、無線ノード１０３から見て、中継ノード１０２はいわゆるＩＥＥＥ１３９４バス側のノードや機能の代理サーバとなっている。無線ノード１０３は、これら（ＩＥＥＥ１３９４側のノードや機能）を中継ノード１０２の機能と考え、通信を行うが、実際には中継ノード１０２が必要なプロトコル変換やデータの乗せ換えを行う。

【００５６】

図４に示されるように、この無線ノード１０３は、無線インタフェース３０１、無線ノード制御パケット送受信部３０２、コピープロテクション処理部３０３、無線ＩＳＯ信号送受信部３０４、受信した暗号化されたストリーム（ＭＰＥＧ映像等）を、コピープロテクション処理部３０３から渡されるコンテンツキーＫを使ってこれを復号化する暗号復号化部３０５、ＭＰＥＧデコード部３０６、映像を表示するディスプレイ部３０７を有する。

【００５７】

無線ノード１０３のコピープロテクション処理部３０３は、後述するように、認証フォーマットＢｃｅｒｔを持ち、その認証の発行機関は、送信ノード１０１（の映像送出サブユニット）の認証フォーマットＡｃｅｒｔの発行機関と同一の発行機関である。

【００５８】

次に、実際のコピープロテクションを施した上でのＭＰＥＧ映像全体のシーケンスについて、図５／図６（全体のシーケンス例）、図７／図８（送信ノード１０１のフローチャート例）、図９／図１０／図１１（中継ノード１０２のフローチャート例）、図１２／図１３（無線ノード１０３のフローチャート例）を参照しながら説明する。

【００５９】

まず、無線ノード１０３は、自分の構成情報を中継ノード１０２に通知する（ステップＳ５０１）。この通知は、無線ノード内にＩＥＥＥ１２１２レジスタを用意し、ここに自分の構成情報を記しておく形で行われてもよい。構成情報とは

、自分（無線ノード）がＭＰＥＧデコード／ディスプレイ機能を持つといったことや、認証・鍵交換のための認証フォーマットを持っていること、などである。ここで、この認証フォーマットが、特定のコピープロテクション機関が定めたフォーマットであることを同時に通知したり、ＩＥＥＥ１３９４向けのコピープロテクションのための認証フォーマットである旨を同時に通知してもよい。

【００６０】

ここで、認証について簡単に説明する。

【００６１】

ネットワーク上を映画やテレビ番組などの著作権を考慮すべきコンテンツ（データ）を転送する場合、それらのコンテンツは暗号によって保護を行うべきである。なぜなら、これらのデータの転送中に、ネットワーク上で盗聴された場合、不正コピーが可能となってしまうからである。これに対する対策としては、転送するデータの暗号化が有効である。

【００６２】

次に問題となるのが、「怪しいものにデータを送っている危険はないか」という問題である。たとえ、データを暗号化して送ったとしても、送った先のノード（暗号を解く鍵を持っている）が悪意を持っている場合（不正コピーをしようと考えている場合）には、やはり解読可能な形でデータを送るべきではない。これに対する対策が認証である。すなわち、この暗号を解く鍵を受信側に渡す前に、受信側が不正を働かないものかどうかの確認をとる（確認が取れた受信側ノードにのみ暗号を解く鍵を渡す）仕組みである。

【００６３】

具体的には、予め認証機関が「このノード（あるいはサブユニット）は、不正に働くことはない」と認定したノード（あるいはサブユニット）に対して、「認証フォーマット」と呼ばれるデータを、あらかじめ送信側のノードと受信側のノードとの両方に与えておく。この「認証フォーマット」を正しい形で持っているということは、そのノード（あるいはサブユニット）は信用できる（不正を働かない）と考えることができる。そこで、上記のデータ転送に先立って、送受信ノード（あるいはサブユニット）間で認証フォーマットのやり取りを行い、正しい

形で認証フォーマットが確認できた場合に限り、暗号を解くための鍵（もしくは鍵を生成するための元となるデータ）を通知し、その鍵で暗号化されたデータをネットワーク上を転送する、という手法をとる。

【００６４】

さて、無線ノード１０３は、このような認証フォーマットをあらかじめ認証機関により与えられており、「暗号化データを正当な形で受信／再生する権利」を持っている。ここで、無線ノード１０３が持っている認証フォーマットを「Ｂｃｅｒｔ」とする。

【００６５】

無線ノード１０３は、図５のステップＳ５０１で自分の構成情報を通知する際に、自分は認証フォーマットを有していることを、この構成情報に加えてもよい（ステップＳ８０１）。例えば、図１４のように、構成情報の中に、本無線ノード１０３がＭＰＥＧデコード／ディスプレイ機能を持っており、さらに該機能が認証フォーマットを持っていること、その認証フォーマットがどの発行機関が発行したものか、等の情報を有する。

【００６６】

なお、中継ノード１０２が無線ノード１０３の構成を認識する方法としては、この他にも中継ノード１０２が無線ノード１０３に対して構成を問い合わせるパケットを送信し、無線ノード１０３がこれに答える方法等も可能である。

【００６７】

さて、この構成情報を受信した中継ノード１０２は、無線ノード１０３が認証フォーマットを持つことや、ＭＰＥＧデコード／ディスプレイ機能を持っていることを確認する（ステップＳ７０１）。

【００６８】

中継ノード１０２は、無線ノード１０３がＭＰＥＧデコード／ディスプレイ機能を持っていることをＩＥＥＥ１３９４バス側のノードに対して知らせるため、このＭＰＥＧデコード／ディスプレイ機能を、中継ノード１０２自身のサブユニットとしてＩＥＥＥ１３９４バス側に広告する（ステップＳ５０２）。具体的には、ＩＥＥＥ１２１２レジスタに「自分はＭＰＥＧデコード／ディスプレイ機能

を持っている」旨を記載したり、ＡＶ／Ｃプロトコルでサブユニット構成の問い合わせを受けた場合に、自分がＭＰＥＧデコード／ディスプレイサブユニットを持っているという形で応答を返したりする（これにより、ＩＥＥＥ１３９４に接続されたノードは、中継ノード１０２にこの機能が存在すると認識することになる）。

【００６９】

そのために、中継ノード１０２は、代理サブユニット構成部２０７内に代理テーブル２０８を持つ。代理テーブル２０８は、図１５／図１６のように、中継ノード１０２が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【００７０】

ここでは、図１５のように、無線ノード１０３のＭＰＥＧデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップＳ７０２，Ｓ７０３）。

【００７１】

このため、送信ノード１０１から見た中継ノード１０２の構造は図１７のように見えることになる（ステップＳ６０１）。

【００７２】

以上は、ＩＥＥＥ１３９４バス側についての説明であったが、これと同様の関係が無線区間にも成り立っている。すなわち、中継ノード１０２は、ＩＥＥＥ１３９４バス側の機器やサービス、サブユニット構成等を調査し、これらの代理サービスを無線区間側に行っている。よって、図１６のような設定がなされ、無線ノードから見た中継ノード１０２の構造は図１８のように見える。

【００７３】

さて、中継ノード１０２内にＭＰＥＧデコード／ディスプレイサブユニットがあると認識した送信ノード１０１は、このサブユニットに対して、ＭＰＥＧ映像を転送することを目的に、１３９４バス上に同期チャネル＃ｘを確立し、ＡＶ／Ｃプロトコルにて「この同期チャネル＃ｘ（を受信するプラグ（例えば１３９４ＴＡにて規定されたＡＶ／Ｃにおけるプラグ））と、ＭＰＥＧデコード／ディス

プレイサブユニットとを接続し、映像を表示せよ」との命令をだす（ステップＳ５０３，Ｓ６０２）。送信ノード１０１は、このサブユニットが中継ノード１０１にあたるものと解釈しているため、命令の送信先は中継ノード１０２である。

【００７４】

これを受信（ステップＳ７０４）した中継ノード１０２は、受信した命令パケットを解釈し、その命令が自らが代理サービスを行っているＭＰＥＧデコード／ディスプレイサブユニットに対する命令であることを認識し、代理テーブル２０８を参照して、この命令先の実体は無線ノード１０３にあることを認識する（ステップＳ７０５）。

【００７５】

よって、ＩＥＥＥ１３９４バスの同期チャネル＃ｘを通して受信したデータを、無線ノード側にフォワードすべく、無線区間の同期チャネル（＃ｙ）の確保を行い（ステップＳ７０６）、さらにＩＳＯ信号送受信部２０４（同期チャネル＃ｘを受信）と無線ＩＳＯ信号送受信部２０５（同期チャネル＃ｙを送信）を接続し、１３９４インタフェース２０１から入力された入力データ（ＩＳＯデータ）を無線区間にフォワードできるようにする（ステップＳ５０４，Ｓ７０７）。

【００７６】

さらに、無線ノード１０３に対して、「無線同期チャネル＃ｙを通してデータを送信するので、これを受信し、ＭＰＥＧデコーダに入力し、その結果をディスプレイに表示せよ」との命令を、無線ノード制御パケットの形で送信する（ステップＳ５０５，Ｓ７０８）。

【００７７】

図１９に、この無線ノード制御パケットの一例を示す。

【００７８】

図１９に示されるように、無線ノード１０３に無線同期チャネル＃ｙを通して送信したデータ（ＭＰＥＧ映像）を、ＭＰＥＧデコード／ディスプレイ機能に転送し、表示することを促す内容となっている。また、この中にこのデータ（ＭＰＥＧ映像）を送信するサブユニット（中継ノード１０２の映像送信機能；実際には、送信ノード１０１の代理でその機能を持っていると広告している）について

の情報も併せて通知している。

【００７９】

これを受信した無線ノード１０３は、無線同期チャネル＃ｙを通してデータが送られてくることを認識する（ステップＳ８０２）。無線ノード１０３は、このデータの送信元は中継ノード１０２の映像送信サブユニットであると認識する（前述のように、実際のデータ送信元は送信ノード１０１である）。このため、この無線ノード制御パケット内に、「この無線同期チャネルを通して送信されるデータの送信元は中継ノード１０２の映像送信サブユニットである」との情報を含めてもよい。

【００８０】

この後、送信ノード１０１は、同期チャネル＃ｘを通して、暗号化されたＭＰＥＧ映像を転送する（ステップＳ６０３，Ｓ５０６）。これを受信した中継ノード１０２は、先に設定したようにこれを無線区間にフォワードする（ステップＳ７０９，Ｓ５０７）。

【００８１】

中継ノード１０２は、ステップＳ５０６で暗号化されたＭＰＥＧ映像を受信した時点で、これが暗号化データであることを認識できるが、無線網側に転送する必要があると認識し、これをそのままフォワードする。後に認証・鍵交換の手続きが必要である旨を記憶しておいてもよい。

【００８２】

このようにして、暗号化されたＭＰＥＧ映像が無線ノード１０３に到達する（ステップＳ８０３）。このＭＰＥＧ映像には、ソースアドレスとして中継ノード１０２のノードＩＤが含まれていてもよい。このため、無線ノード１０３は、このＭＰＥＧ映像が中継ノード１０２から到達したものであることまでは認識できるが、この時点で無線ノード１０３はこの暗号を解くための鍵Ｋを有していない（もしくはその鍵を生成するための元となるデータを有していない）ため、この状態で暗号を解いて、ＭＰＥＧ映像を取り出すことはできない。ここで、無線ノード１０３は認証手続きがＭＰＥＧ映像の送信元と必要であることを認識する。

【００８３】

そこで、無線ノード１０３（のコピープロテクション処理部３０３）は、認証要求を暗号化データの送信元に対して送信する。先に述べたように、無線ノード１０３には、上記暗号化データの送信元は中継ノード１０２（内の、サブユニット種別＝映像送信サブユニット、かつ、サブユニットＩＤ＝ｂ（ｂ＝０とする）の、サブユニット）であるように認識されている。

【００８４】

また、図５のＳ５２１のように、中継ノード１０２に対して、「無線ノードにおいて、無線同期チャネル＃ｙを受信しているのは、サブユニット種別＝ＭＰＥＧデコード／ディスプレイサブユニットで、かつ、サブユニットＩＤ＝ｃ（ｃ＝０とする）の、サブユニットである。無線同期チャネル＃ｙに暗号化データを送信しているのはどのサブユニットか？」という意味合いの問い合わせを送信してもよい。これに対し、中継ノード１０２は、「無線同期チャネル＃ｙに送信しているのは、映像送信サブユニットのサブユニットＩＤ＝０である。」との返答を返す（ステップＳ５２２，Ｓ７３１，Ｓ８３１）。これにより、無線ノード１０３は、認証を行なう先が中継ノードの映像送信サブユニットであることを認識できる。

【００８５】

このように、認証要求の宛先を認識し、中継ノード１０２（内の映像送信サブユニットのサブユニットＩＤ＝０）に対し、認証要求を送信する。この送信の仕方として、認証要求パケットの宛先を「中継ノードの映像送信サブユニット（のサブユニットＩＤ＝０）」としてもよいし、認証要求パケットの任意の位置に「映像送信サブユニット（のサブユニットＩＤ＝０）」という情報を入れ、認証要求先は映像送信サブユニット（のサブユニットＩＤ＝０）であると言うことを明確に表示してもよい。前者の場合は、中継ノードの各サブユニット内に認証・鍵交換の手続きが含まれていることを意味する。後者の場合は、中継ノードのある特定の処理部が、一括して、各サブユニットの認証・鍵交換を行なうことを意味する。

【００８６】

その際、認証要求には、無線ノード１０３の認証フォーマットＢｃｅｒｔを付

与する（ステップＳ８０４，Ｓ５０８）。Ｂｃｅｒｔは、無線ノード１０３のＭＰＥＧデコード／ディスプレイサブユニットの認証フォーマットであってもよい。なお、コピープロテクション処理部は、サブユニット毎（サブユニット種別毎）でなく、サブユニットＩＤ毎に認証フォーマットを用意してもよい。

【００８７】

認証要求を受信（ステップＳ７１０）した中継ノードは、代理テーブル２０８を参照して、この認証要求の要求先が実は送信ノード１０１（の映像送信サブユニットのサブユニットＩＤ＝ａ（ａ＝０とする））であることを認識する。

【００８８】

中継ノード１０２は、送信ノード１０１に対して、「中継ノードにおいて、同期チャネル＃ｘを受信しているのはＭＰＥＧデコード／ディスプレイサブユニットのサブユニットＩＤ＝０である。同期チャネル＃ｘに暗号化データを送信しているのは、送信ノードのどのサブユニットか？」という意味合いの問い合わせを送信してもよい（ステップＳ５２３，Ｓ６３１，Ｓ７３２）。これに対し、送信ノード１０１は、「同期チャネル＃ｘに送信しているのは、映像送信サブユニットのサブユニットＩＤ＝０である。」との返答を返す（ステップＳ５２４，Ｓ６３１，Ｓ７３２）。

【００８９】

このようにして、認証要求の相手を認識したならば、ステップＳ５０８にて受信した認証要求を、中身を変えずに（Ｂｃｅｒｔ等はそのまま残して）送信ノード１０１に対してフォワードする（ステップＳ５０９，Ｓ７１１）。すなわち、宛先アドレスや、認証要求の宛先であるサブユニット以外の認証フォーマット等は、中継ノードは透過的に転送できる。

【００９０】

認証要求の転送の際は、先に説明したように、認証要求パケットの宛先を映像送信サブユニット（のサブユニットＩＤ＝０）としてもよいし、認証要求パケットの任意の位置に当該サブユニットを明示する情報を入れ、認証要求先は当該サブユニットであると言うことを明確に表示してもよい。

【００９１】

ここで、認証要求の中身を変えずにフォワードすることで、この認証要求はそのままの形で送信ノード１０１に到達することになり、結局、送信ノード１０１と無線ノード１０３との間で、実際の認証手続きは進んでいくことになり、しかも中継ノード１０２をはじめ、その他のノードにはその認証の結果明らかになる鍵の値などの情報を知られることなく、以上の手続きを行っていくことが可能である。

【００９２】

認証要求を受け取った送信ノード１０１は、これを中継ノード１０２のＭＰＥＧデコード／ディスプレイサブユニットから送られてきた認証要求であると解釈する（ステップＳ６０４）。その後、Ｂｃｅｒｔから無線ノード１０３のＭＰＥＧデコード／ディスプレイサブユニットを特定できるＩＤ（Ｂｄｉｄ）を抽出し（ステップＳ６０５）、これとともに、やはり同様の認証要求を認証要求の送信元に対して行おうとする。ただし、送信ノード１０１は、Ｂｃｅｒｔが無線ノード１０３の認証フォーマットであるとは意識することはなく、むしろ中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）の認証フォーマットであると意識をしている。

【００９３】

この認証要求には、送信ノード１０１（の映像送出サブユニット）の認証フォーマットＡｃｅｒｔと、Ｂｄｉｄとが含まれる。ここで、送信ノード１０１は、該認証要求（ステップＳ５０９）の送信元は中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）であると解釈しているため、この認証要求の送信先はやはり中継ノード１０２となる（ステップＳ６０６，Ｓ５１０）。

【００９４】

これを受信（ステップＳ７１２）した中継ノード１０２は、代理テーブル２０８を参照して、この認証手続の本来の要求先が無線ノード１０３（のＭＰＥＧデコード／ディスプレイ機能）であることを認識し、この認証手続要求を、中身を変えずに（Ａｃｅｒｔ等はそのまま残して）無線ノード１０３に対してフォワードする（ステップＳ５１１，Ｓ７１３）。この認証要求の送信元は中継ノード１０２である。

【００９５】

これを受け取った無線ノード１０３は、これを中継ノード１０２の映像送信サブユニットから送られてきた認証要求であると解釈する（ステップＳ８０５）。その後、Ａｃｅｒｔから送信ノード１０１の映像サブユニットを特定できるＩＤ（Ａｄｉｄ）を抽出し、認証鍵の交換に必要な残りの手続きを、認証要求の送信元に対して行おうとする。なお、この場合も、無線ノード１０３は、Ａｃｅｒｔが送信ノード１０１の認証フォーマットであるとは意識せず、むしろ中継ノード１０２（の映像送信サブユニット）の認証フォーマットであると意識する。

【００９６】

この認証鍵の交換に必要な残りの手続きとして、無線ノード１０３は、認証要求の送信元（と無線ノードが解釈しているノード）に対して認証・鍵交換手続きパケットを送信する（ステップＳ５１２）。この認証・鍵交換手続きパケットには、鍵交換初期値、署名、Ａｃｅｒｔの中に含まれていた送信ノード（の映像送信サブユニット）のデバイスＩＤ（Ａｄｉｄ）等が含まれている（ステップＳ８０６）。ここで、無線ノード１０３は、該認証要求（ステップＳ５１１）の送信元は中継ノード１０２（の映像送信サブユニット）であると解釈しているため、この認証要求の送信先はやはり中継ノード１０２となる。

【００９７】

これを受信した中継ノード１０２は、代理テーブル２０８を参照して、この認証手続きの本来の要求先が送信ノード１０１（の映像送信サブユニット）であることを認識し、この認証手続きパケットを、中身を変えずに送信ノード１０１に対してフォワードする（ステップＳ５１３，Ｓ７１４）。このパケットの送信元は中継ノード１０２である。

【００９８】

これと同様の手続きが送信ノード１０１→中継ノード１０２→無線ノード１０３の方向に対しても行われる（ステップＳ５１４，Ｓ５１５，Ｓ６０９，Ｓ７１５，Ｓ８０７）。

【００９９】

この認証手続きパケットを受信した送信ノード１０１および無線ノード１０３

は、それぞれ、受信したパケットが改ざんされていないかどうかのタンパの確認、相手から送られてきた認証フォーマットが正しいものであるかどうかの確認等を行い、与えられた値を使って共通の認証鍵Ｋａｕｔｈを導き出す。この共通の認証鍵Ｋａｕｔｈは、送信ノード（の映像送信サブユニット）と無線ノード（のＭＰＥＧデコード／ディスプレイ機能）との間で共通に持つ鍵で、この鍵Ｋａｕｔｈを、この両者（送信ノード１０１、無線ノード１０３）以外の他人に知られることなく共有することがこの時点でできるようになる（ステップＳ６０７，ステップＳ６０８，Ｓ８０８）。

【０１００】

この認証鍵Ｋａｕｔｈを使って、実際にＭＰＥＧストリームの暗号化を行うコンテンツキーＫの計算ができるようになる。具体的な手順はここでは省略するが、送信ノード１０１から無線ノード１０２に、ＩＥＥＥ１３９４のコピープロテクション方式（５Ｃ方式）のように、交換鍵やシード（種）の値を別途送ることにより、コンテンツキーＫの計算ができるようになっていてもよい（ステップＳ５１８，Ｓ５１９）。

【０１０１】

さて、このようにして、送信ノード１０１（の映像送信サブユニット）と無線ノード１０３（のＭＰＥＧデコード／ディスプレイ機能）との間で、コンテンツキーＫの値が共有できるようになった。

【０１０２】

ここで、送信ノード１０１が、送信するＭＰＥＧ映像を、コンテンツキーＫを使って、暗号化部４０５にて暗号化し（ステップＳ６１０）、これを１３９４バスの同期チャネル＃ｘを通して中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）に対して送信する（ステップＳ５１６，Ｓ６１１）。

【０１０３】

中継ノード１０２は、送信ノード１０１から同期チャネル＃ｘを通して送られてくる暗号化されたＭＰＥＧ映像を、ＩＳＯ信号送受信部２０４から無線ＩＳＯ信号送受信部２０５を通して、無線同期チャネル＃ｙに送信する（ステップＳ５１７，Ｓ７１６）。

【０１０４】

これを受信した無線ノード１０３は、キーＫの値を使ってＭＰＥＧ映像の値を復号化する（ステップＳ８０９，ステップＳ８１０）。復号化されたＭＰＥＧデータは、ＭＰＥＧデコード部３０６にて復号化され（ステップＳ８１１）、これをディスプレイ部３０７にて再生表示する（ステップＳ８１２）。

【０１０５】

このように、１３９４バスと無線網との間に代理ノードが存在するような相互接続の環境においても、エンドーエンドのノード同士（本実施形態では送信ノード１０１と無線ノード１０３）が認証手続きや鍵交換手続きを行うことができ、さらにその内容を中継ノード１０２を含め、その他のノードが知ることはできない仕組みとなっている。また、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送も、コピーが不可能なように経路の全てで暗号化されており、安全なデータ転送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【０１０６】

なお、以上の実施形態は、認証手続きや、暗号鍵の交換手続き等を、ノードのサブユニット単位で行ってきたが、無線ノード単位でこれを行うことも可能である。なお、ノード単位で行う例については、次の第２の実施形態で説明するので、例えばこれを適用すればよい。

【０１０７】

また、以上の実施形態では、認証および鍵交換のための手続きを暗号化データの受信後に行ってきたが、該手続きは、暗号化データ受信に先だって行ってももちろん構わない。例えば、装置や該当アプリケーションの立ち上げ時に該手続きを行ってもよい。

【０１０８】

（第２の実施形態）

次に、第２の実施形態について説明する。

【０１０９】

第１の実施形態では、送信ノードと無線ノードとが、直接、互いに認証手続きや鍵交換手続きを行ってきた。すなわち、送信ノード（の映像サブユニット）と無線ノード（のＭＰＥＧデコード／ディスプレイ機能）とが、直接、互いを認証し、暗号鍵の交換手続きを行って、暗号化データのやり取りを行ってきた。この際、中継ノードは、送信ノードに対しては無線ノードのＭＰＥＧデコード／ディスプレイ機能の代理機能を果たし、無線ノードに対しては送信ノードの映像送信サブユニットの代理機能を果たしてきたが、上記の認証手続きおよび暗号化データのやり取りの部分については、これらのデータの単なるフォワードを、代理していたサブユニットなり機能なりに行う形であった。

【０１１０】

これに対し、第２の実施形態では、中継ノードにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを終端する場合の例を示す。すなわち、送信ノードと中継ノードとの間、および中継ノードと無線ノードとの間で、各々のコピープロテクション手続きは閉じている。つまり、この実施形態においても、中継ノードは、送信ノードあるいは無線ノードに対して代理サービスは提供するものの、コピープロテクションについては、中継ノード自身が認証フォーマットを持ち、中継ノード自身が、１３９４バス区間のＭＰＥＧデータの暗号化転送についての責任を終端するとともに、無線区間のＭＰＥＧデータの暗号化転送についての責任を終端する場合の例である。

【０１１１】

図２０に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第１の実施形態と同様である。

【０１１２】

図２１に、送信ノード２１０１の内部構造の一例を示す。これも第１の実施形態と基本的には同様である。

【０１１３】

次に、図２２に、中継ノード２１０２の内部構造の一例を示す。

【０１１４】

中継ノード２１０２は、第１の実施形態と同様に、ＩＥＥＥ１３９４バス側の

ノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対してＩＥＥＥ１３９４バス側のノード（本実施形態では送信ノード２１０１）の代理サーバとなり、ＩＥＥＥ１３９４バス側のノードの機能を代理で提供する機能を持つ。

【０１１５】

また、ＩＥＥＥ１３９４バス側から受信したデータ（ＭＰＥＧ映像データ）を無線区間側にフォワードする機能を持つが、第１の実施形態と相違する点は、認証データや暗号化等、コピープロテクションに関する手続きがＩＥＥＥ１３９４バス区間と無線区間との両方について、この中継ノード２１０２において終端されており、ＩＥＥＥ１３９４バス側については認証フォーマットＢｃｅｒｔをＩＥＥＥ１３９４コピープロテクション処理部２２０８に、無線区間側については認証フォーマットＣｃｅｒｔを無線区間コピープロテクション処理部２２１２にそれぞれ持ち、１３９４バスの同期チャネルから入力されてきた暗号化データについては、ＩＳＯ信号受信部２２０３にて受信→暗号復号化部２２０４にて暗号復号化→復号化されたＭＰＥＧ映像を、暗号化部２２０５にて再暗号化→無線ＩＳＯ信号送受信部２２０６にて、無線同期信号上に送信、というプロセスを踏む点である。

【０１１６】

これらの認証フォーマットは、ＩＥＥＥ１３９４インタフェース毎、あるいは無線区間インタフェース毎に１つずつもっていてもよいし、（代理も含めて）サブユニット毎（サブユニット種別毎）に１つずつ持っていてもよい。

【０１１７】

ここで、ＡｃｅｒｔとＢｃｅｒｔは、同じ認証機関（例えばＩＥＥＥ１３９４のコピープロテクションを担当する認証機関）が発行した認証フォーマットであると仮定するが、後述する無線区間の認証フォーマット（後述するＣｃｅｒｔとＤｃｅｒｔ）については、同じくこの認証機関が発行したものであってもよいし、無線区間を担当する別の認証機関が発行する認証フォーマットであってもよい。

【０１１８】

次に、図２３に、無線ノード２１０３の内部構造の一例を示す。コピープロテクション処理部２３０３が、無線区間向けの認証フォーマットＤｃｅｒｔを持っていること以外は、基本的には第１の実施形態の無線ノードと同様である。

【０１１９】

次に、実際のコピープロテクションを施した上でのＭＰＥＧ映像全体のシーケンスについて、図２４／図２５（全体のシーケンス例）、図２６／図２７（送信ノード２１０１のフローチャート例）、図２８／図２９／図３０／図３１（中継ノード２１０２のフローチャート例）、図３２／図３３（無線ノード２１０３のフローチャート例）を参照しながら説明する。

【０１２０】

まず、無線ノード２１０３は、自分の構成情報を中継ノード２１０２に通知する（ステップＳ２５０１）。構成情報とは、自分（無線ノード）がＭＰＥＧデコード／ディスプレイ機能を持つことといったことや、認証のための認証フォーマットを持っていることなどである（図１４参照）。ここで、認証のための認証フォーマットが、無線区間用の認証フォーマットである旨を通知してもよい（ステップＳ２８０１）。

【０１２１】

これを受信した中継ノード２１０２は、無線ノード２１０１が認証フォーマットを持つことや、ＭＰＥＧデコード／ディスプレイ機能を持っていることを確認する（ステップＳ２７０１）。中継ノード２１０２は、第１の実施形態と同様に、このＭＰＥＧデコード／ディスプレイ機能を、ＩＥＥＥ１２１２レジスタやＡＶ／Ｃプロトコル等を使って、中継ノード２１０２自身のサブユニットとしてＩＥＥＥ１３９４バス側に広告する（ステップＳ２５０２）。

【０１２２】

そのために、中継ノード２１０２は、代理サブユニット構成部２２１０内に代理テーブル２２１４を持つ。この代理テーブル２２１４は、基本的には第１の実施形態と同様であり、図３４／図３５のように、中継ノード２１０２が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【０１２３】

ここでは、図３４のように、無線ノード２１０３のＭＰＥＧデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップＳ２７０２，Ｓ２７０３）。

【０１２４】

このため、送信ノード２１０１から見た中継ノード２１０２の構造は、図３６のように見えることになる（ステップＳ２６０１）。

【０１２５】

以上は、ＩＥＥＥ１３９４バス側についての説明であったが、第１の実施形態と同様に、これと同様の関係が無線区間にも成り立っている。すなわち、中継ノード２１０２は、ＩＥＥＥ１３９４バス側の機器やサービス、サブユニット構成等を調査し、これらの代理サービスを無線区間側に行っている。よって、図３５のような設定がなされ、無線ノードから見た中継ノード２１０２の構造は図３７のように見える。

【０１２６】

さて、中継ノード２１０２内にＭＰＥＧデコード／ディスプレイサブユニットがあると認識した送信ノード２１０１は、このサブユニットに対して、ＭＰＥＧ映像を転送することを目的に、１３９４バス上に同期チャンネル＃ｘを確立し、ＡＶ／Ｃプロトコルにて「この同期チャネル＃ｘ（を受信するプラグ）と、ＭＰＥＧデコード／ディスプレイサブユニットとを接続し、映像を表示せよ」との命令を出す（ステップＳ２５０３，Ｓ２６０２）。送信ノード２１０１は、このサブユニットが中継ノード２１０２にあるものと解釈しているため、命令の送信先は中継ノード２１０２である。

【０１２７】

これを受信（ステップＳ２７０４）した中継ノード２１０２は、受信した命令パケットを解釈し、その命令が自らが代理サービスを行っているＭＰＥＧデコード／ディスプレイサブユニットに対する命令であることを認識し、代理テーブル２２１０を参照して、この命令先の実体は無線ノード２１０３にあることを認識する（ステップＳ２７０５）。

【０１２８】

ここで、図２０の無線区間は、ＱＯＳ対応の無線ＬＡＮになっており、予め定められた手順を踏めば、パケット廃棄や遅延等の品質劣化無く、転送データを送信先まで転送することが可能であるとする。この無線ＬＡＮ上では、データは図３８のように、イーサネットフレームと同様のフォーマット、すなわち「送信元アドレス、宛先アドレス、データ」のようなフォーマットを持つ、無線フレームで転送される。

【０１２９】

さて、ＩＥＥＥ１３９４バスの同期チャネル＃ｘを通して受信したデータを、無線ノード側にフォワードすべく、無線区間のＱＯＳ設定を行う。さらにＩＳＯ信号送受信部２２０３（同期チャネル＃ｘを受信）と無線ＩＳＯ信号送受信部２２０６（ＱＯＳ保証を行なう無線フレームにて送信）を図２２の点線のように接続し（まだ暗号の復号化ができないため）、１３９４インタフェース２２０１から入力されたＩＳＯ入力データを無線区間にそのままフォワードできるようにしてもよい（ステップＳ２５０４，Ｓ２７０６，Ｓ２７０７）。

【０１３０】

さらに、無線ノード２１０３に対して、「上記無線フレームを通して、データを送信するので、これを受信し、その結果をディスプレイに表示せよ」との命令を無線ノード制御パケットの形で送信する（ステップＳ２５０５，Ｓ２７０８，Ｓ２８０２）。この制御プロトコルには、ＩＥＥＥ１３９４ＡＶ／Ｃプロトコル、あるいはＩＥＣ６１８８３プロトコルや、これらを変形したものを用いてもよい。後述するように、本実施形態では、無線ＬＡＮ上に同期チャネルの概念はないものの、転送するデータにソースＩＤ（ＳＩＤ）なる領域を設け、無線区間にＱＯＳデータを送信しているノード毎に、転送しているＱＯＳデータを一意に区別できるようになっており、このＳＩＤの値をＩＥＥＥ１３９４の同期チャネルのように、データフローの判別に用いることができる。無線ノード制御パケットの一例を図３９に示す。パケットの送信元は中継ノード２１０２である。

【０１３１】

これを受信した無線ノード２１０３は、αなるＳＩＤが付与されて、データがＱＯＳ転送されてくることを認識する。

【０１３２】

この後、送信ノード２１０１は、同期チャネル＃ｘを通して、暗号化されたＭＰＥＧ映像を転送する（ステップＳ２５０６，Ｓ２６０３）。コンテンツ鍵はＫ１とする。この暗号鍵は、後述する交換鍵やシードの関数として導出される。

【０１３３】

また、この暗号化されたＭＰＥＧ映像を送信するフレームには、同期チャネル番号の他、送信ノードを識別する「送信ノードＩＤ」が含まれていてもよい。

【０１３４】

これを受信した中継ノード２１０２は、データが暗号化されていることを認識するとともに、例えば受信データに含まれる「送信ノードＩＤ」を参照して、このデータを送信しているのが送信ノード２１０１であることを認識し（ステップＳ２７０９）、送信ノード２１０１に対して、「同期チャネル＃ｘを通して、このデータを送出しているのは、送信ノード２１０１のどのサブユニットか」を確かめるため、認証先の問合せを行なう（ステップＳ２５０７，Ｓ２７１０）。この際、データが転送されている同期チャネル番号（＃ｘ）を記載して、送信ノード２１０１が、データを送信しているサブユニットを特定できるようにしておくとともに、このデータを受信する自身のサブユニット（本実施形態の場合、中継ノード２１０２のＭＰＥＧデコード／ディスプレイサブユニットのサブユニットＩＤ＝０）も通知する。これは、送信ノード２１０１から見た認証先を通知する役割を持つ。

【０１３５】

なお、この認証先問合せパケットと、後述する認証先応答パケットは、認証機関のプライベート鍵でハッシュや暗号化したデータを電子署名として記載しておき、改ざん等が無いことを確認できるようにしてもよい。

【０１３６】

さて、認証先問合せを受信（ステップＳ２６０４）した送信ノード２１０１は、同期チャネル＃ｘに対して送信しているデータを受信しているサブユニットが、中継ノード２１０２のＭＰＥＧデコード／ディスプレイサブユニットであることを認識するとともに、自らが該同期チャネル＃ｘに送信しているサブユニット

が、映像送信サブユニット（サブユニットＩＤ＝０）であることを、認証先応答パケットとして、中継ノード２１０２に通知する（ステップＳ２５０８，Ｓ２６０５）。

【０１３７】

これにより、中継ノード２１０２は、同期チャネル＃ｘにデータを送信しているサブユニットが、送信ノード２１０１の映像送信サブユニット（サブユニットＩＤ＝０）であることを認識できる（ステップＳ２７１１）。

【０１３８】

同期チャネル＃ｘにデータを送信しているサブユニットが、送信ノード２１０１の映像送信サブユニットであることを認識した中継ノード２１０２（のＭＰＥＧデコード／ディスプレイサブユニットの代理機能）は、続いて送信ノード２１０１の映像送信サブユニットに対して認証要求を行なう。この認証要求には、中継ノード、あるいは中継ノードのＭＰＥＧデコード／ディスプレイサブユニットの認証フォーマット（Ｂｃｅｒｔ）が共に転送される（ステップＳ２５０９，Ｓ２６０６，Ｓ２６０７，Ｓ２７１２）。この認証要求と認証フォーマットの交換は、第１の実施形態と同様に、送信ノード２１０１（の映像送信サブユニット）から中継ノード２１０２（のＭＰＥＧデコード／ディスプレイサブユニット）に向けても行われる（ステップＳ２５１０，Ｓ２６０８，Ｓ２７１３，Ｓ２７１４）。このように、第２の実施形態においても、認証・鍵交換にサブユニットに関する情報も交換するのは、同じ装置同士の通信でも、通信しているサブユニットが異なれば、異なる鍵の使用ができるようにするためである。

【０１３９】

お互いに認証が完了した両ノードは、第１の実施形態と同様に認証・鍵交換手続きを行い（ステップＳ２５１１１，Ｓ２５１１２，Ｓ２６０９，Ｓ２７１５）、認証鍵Ｋａｕｔｈ１を共有する。この認証鍵を使って、送信ノード２１０１は、交換鍵やシードの転送を中継ノード２１０２に対して行ない（ステップＳ２５１２，Ｓ２６１０，，Ｓ２７１６）、結局、中継ノード２１０２では、コンテンツ鍵Ｋ１の値を知ることができるようになる（ステップＳ２７１７）。

【０１４０】

以降、転送されてくるコンテンツ鍵Ｋ１で暗号化されたＭＰＥＧ映像（同期チャネル＃ｘ経由）（ステップＳ２５１３，Ｓ２６１１，Ｓ２６１２）は、中継ノード２１０２にて復号化され（ステップＳ２５１４，Ｓ２７１８）、さらに無線区間用に別に用意されたコンテンツ鍵ｋ２で再暗号化され（ステップＳ２５１５，Ｓ２５１６，Ｓ２７１９）、無線区間上をＱＯＳが保証される形で、無線ノード２１０３に対して送信される（ステップＳ２５１７，Ｓ２７２０，Ｓ２８０３）。この時点では、ＭＰＥＧ映像はＩＳＯ信号送受信部２２０３、暗号復号化部２２０４、暗号化部２２０５、無線ＩＳＯ信号送受信部２２０６というパスを通る。

【０１４１】

先に述べたように、このとき中継ノード２１０２が、無線区間側に送信しているデータの区別ができるようにするために、ソースＩＤなる、中継ノード２１０２で一意な値を付与して送出してもよい。ここでは、この一意な値をαとする。すなわち、αの値のついたデータは、ＩＥＥＥ１３９４の同期チャネル＃ｘから受信したデータ（をコンテンツ鍵Ｋ１で復号化し、コンテンツ鍵Ｋ２で再暗号化したもの）である。中継ノード２１０２は、αのＳＩＤを付けて無線区間に送出しているデータは、自身の無線区間側の映像送信サブユニットの代理機能から送信しているデータであることを認識している。

【０１４２】

これを受信した無線ノード２１０３の動作は、基本的に先に説明した、暗号化データを受信した中継ノード２１０２の動作と同様である。すなわち、データが暗号化されていることを認識するとともに、例えば受信データに含まれる「送信元アドレス」を参照して、このデータを送信しているのが中継ノード２１０２であることを認識し、中継ノード２１０２に対して、「αなる値を付与して、このデータを送出しているのは、中継ノード２１０２のどのサブユニットか」を確かめるため、中継ノードに認証先の問合せを行なう（ステップＳ２５１８，Ｓ２８０４）。

【０１４３】

この際、データが転送されているＳＩＤの値（α）を記載して、中継ノード２

１０２が、データを送信しているサブユニットを特定できるようにしておくとともに、このデータを受信する受信側のサブユニット（本実施形態の場合、無線ノード２１０３のＭＰＥＧデコード／ディスプレイサブユニットのサブユニットＩＤ＝０）も通知する。これは、中継ノード２１０２から見た認証先を通知する役割を持つ。

【０１４４】

認証先問合せを受信（ステップＳ２７２１）した中継ノード２１０２は、ＳＩＤ＝αに対して送信しているデータを受信しているサブユニットが、無線ノード２１０３のＭＰＥＧデコード／ディスプレイサブユニット（サブユニットＩＤ＝０）であることを認識するとともに、自らがＳＩＤ＝αを付与して送信しているサブユニットが、映像送信サブユニットであることを、認証先応答パケットとして、無線ノード２１０３に通知する（ステップＳ２５１９，Ｓ２７２２，Ｓ２８０５）。

【０１４５】

これにより、無線ノード２１０３は、ＳＩＤ＝αを付与してデータを送信しているサブユニットが、中継ノード２１０２の映像送信サブユニットであることを認識できる。

【０１４６】

ＳＩＤ＝αを付与してデータを送信しているサブユニットが、中継ノード２１０２の映像送信サブユニットであることを認識した無線ノード２１０３（のＭＰＥＧデコード／ディスプレイサブユニット）は、続いて中継ノード２１０２の映像送信サブユニットに対して認証要求を行なう（ステップＳ２５２０，Ｓ２７２３，Ｓ２７２４，Ｓ２８０６）。この認証要求には、無線ノード（または無線ノードのＭＰＥＧデコード／ディスプレイサブユニット）の認証フォーマット（Ｄｃｅｒｔ）が共に転送される。この認証要求と認証フォーマットの交換は、中継ノード２１０２（の映像送信サブユニット）から無線ノード２１０３（のＭＰＥＧデコード／ディスプレイサブユニット）に向けても行われる（ステップＳ２５２１，Ｓ２７２５，Ｓ２８０７）。

【０１４７】

お互いに認証が完了した両ノードは、続いて認証・鍵交換手続きを行い（ステップＳ２５２２，Ｓ２５２３，Ｓ２７２６，Ｓ２８０８）、認証鍵Ｋａｕｔｈ２を共有する。この認証鍵を使って、中継ノード２１０２は、交換鍵やシードの転送を無線ノード２１０３に対して行い（ステップＳ２５２４，Ｓ２７２７，Ｓ２８０９）、結局、無線ノード２１０３で、コンテンツ鍵Ｋ２の値を知ることができるようになる（ステップＳ２８１０）。

【０１４８】

なお、これまでの説明では送信ノードと中継ノード間の認証・鍵交換と、中継ノードと無線ノード間の認証・鍵交換とは、順次行われる形で説明したが、逆の順番でもよいし、両者を並行して行うことも可能である。

【０１４９】

以降、転送されてくるコンテンツ鍵Ｋ１で暗号化されたＭＰＥＧ映像（ステップＳ２５２５）は、中継ノード２１０２にて復号化され（ステップＳ２５２６）、さらに無線区間用に別に用意されたコンテンツ鍵Ｋ２で再暗号化され（ステップＳ２５２７，Ｓ２５２８，Ｓ２７２８）、無線区間上をＱＯＳが保証される形で、ＳＩＤ＝αが付与された無線フレームの形で無線ノード２１０３に対して送信される（ステップＳ２５２９，Ｓ２７２９）。

【０１５０】

今度は、無線ノード２１０３は、先に入手した交換鍵、シードの値を使って、コンテンツ鍵Ｋ２を計算できるので、これを復号化することが可能であり（ステップＳ２５３０，Ｓ２８１１）、これをディスプレイ部２３０７にて再生する（ステップＳ２８１２）。

【０１５１】

このように、ＩＥＥＥ１３９４バスと無線網のと間に代理ノードが存在するような相互接続の環境においても、代理機能を提供する中継ノードと送信ノード、および中継ノードと受信ノードが、それぞれの区間で、認証手続きや鍵交換手続きを行うことで、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。これによって、このような相互接続の環境にお

いても、コピープロテクションを考慮したデータ転送が可能になる。

【０１５２】

もちろん、中継ノード２１０２の「生のＭＰＥＧデータ」が流れる部分、具体的には暗号復号化部２２０４と暗号化部２２０５との間には、データをコピーされる危険が考えられるため、この部分でデータコピーがなされないようにするための工夫（例えば、暗号復号化部と暗号化部を一体のＬＳＩにするなど）がなされていると、この間でプローブをあてるなどしてデータを盗聴（不正コピー）することが実質的に不可能になるため、このような対策を行っておくことが有益である。

【０１５３】

（第３の実施形態）

次に、第３の実施形態について説明する。

【０１５４】

第３の実施形態では、ＩＥＥＥ１３９４上において、ＨＡＶｉ規格（Ｓｐｅｃｉｆｉｃａｔｉｏｎ ｏｆ ｔｈｅ Ｈｏｍｅ Ａｕｄｉｏ／Ｖｉｄｉｏ Ｉｎｔｅｒｏｐｅｒａｂｉｌｉｔｙ（ＨＡＶｉ） Ａｒｃｈｉｔｅｃｔｕｒｅ）等に代表される、ＡＶ／Ｃの上位レイヤに相当するＡＶ機器制御ソフトウェアが稼働している場合における実施形態である。

【０１５５】

図４０に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第１の実施形態と同様である。

【０１５６】

図４１に、送信ノード４１０１の内部構造の一例を示す。これも第１の実施形態の場合とほぼ同様であるが、ＩＥＥＥ１２１２レジスタ４４０７を強調のため、追加記述している。ＩＥＥＥ１２１２レジスタ４４０７には、送信ノード４１０１の属性、例えば「どのベンダの製品かを示す情報、例えばＶＴＲやチューナ等といったどのようなジャンルの製品かを示す情報、製造番号、制御ソフトウェアの配置ＵＲＬ、制御アイコン、コマンド一覧」等の情報が含まれる。

【０１５７】

次に、図４２に、中継ノード４１０２の内部構造の一例を示す。中継ノード４１０２も、第１の実施形態とほぼ同様の構成であるが、本実施形態のシーケンスを説明する際に必要なＩＥＥＥ１２１２レジスタ４２１３を１３９４バス構成認識部４２０６内に特に記した点と、ＨＡＶｉ処理部４２１２を持つ点が第１の実施形態と異なる。ＨＡＶｉ処理部４２１２には、いわゆるＨＡＶｉバイトコードの処理を行う仮想マシン（ＶＭ）が存在する。また、本実施形態においては、制御画面の記述を行う「パネルサブユニット」の代理機能を代理サブユニット構成部４２０７が持つ。

【０１５８】

次に、図４３に、無線ノード４１０３の内部構造の一例を示す。これについても、第１の実施形態の場合と基本的には同様である。

【０１５９】

次に、ＨＡＶｉ環境における、実際のコピープロテクションを施した上でのＭＰＥＧ映像全体のシーケンスについて、図４４／図４５（全体のシーケンス例）、図４６／図４７（送信ノード４１０１のフローチャート例）、図４８／図４９／図５０（中継ノード４１０２のフローチャート例）、図５１／図５２（無線ノード４１０３のフローチャート例）を参照しながら説明する。

【０１６０】

まず、無線ノード４１０３は、自分の構成情報を中継ノード４１０２に通知する（ステップＳ４５０１）。このとき、これらの構成情報は、ＩＥＥＥ１２１２レジスタ形式の情報として中継ノード４１０１に送付するものとする。すなわち、中継ノード４１０２が、無線ノード４１０３に対して「ＩＥＥＥ１２１２で規定されるＣＳＲ（コマンド・ステータスレジスタ）空間の、このアドレスに相当する部分についての情報」を要求し、これに無線ノード４１０３が答える形でこのやり取りが行われてもよい。ここで、前述のように、この構成情報には、自分（無線ノード）がＭＰＥＧデコード／ディスプレイ機能を持つといったことや、認証のための認証フォーマットを持っていること、等が含まれる。ここで、無線ノード４１０３が持っている認証フォーマットをＢｃｅｒｔとする。

【０１６１】

これを受信した中継ノード４１０２は、無線ノード４１０１が認証フォーマットを持つことや、ＭＰＥＧデコード／ディスプレイ機能を持っていることを確認する（ステップＳ４７０１）。中継ノード４１０２は、無線ノード４１０１がＭＰＥＧデコード／ディスプレイ機能を持っていることをＩＥＥＥ１３９４バス側のノードに対して知らせるため、このＭＰＥＧデコード／ディスプレイ機能を、中継ノード４１０２自身のサブユニットとしてＩＥＥＥ１３９４バス側に広告する（ステップＳ４５０２）。具体的には、自身のＩＥＥＥ１２１２レジスタに「自分はＭＰＥＧデコード／ディスプレイ機能を持っている」旨を記載したり、ＡＶ／Ｃプロトコルでサブユニット機能の問い合わせを受けた場合に、自分がＭＰＥＧデコード／ディスプレイサブユニットを持っているという形で応答を返したりする（これにより、送信ノード４１０１等のＩＥＥＥ１３９４に接続されたノードは、中継ノードにこの機能が存在すると認識することになる）。

【０１６２】

そのために、中継ノード４１０２は、代理テーブル４２０８を持つ。代理テーブル４２０８は、図５３／図５４のように、中継ノード４１０２が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【０１６３】

ここでは、図５３のように、無線ノード４１０３のＭＰＥＧデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップＳ４７０２，Ｓ４７０３）。

【０１６４】

以上と逆の手続きがＩＥＥＥ１３９４バス４１０４上の送信ノード４１０１の代理登録を無線区間側に対してみせる形で行われる（ステップＳ４５０３，Ｓ４５０４）。すなわち、送信ノード４１０１のＩＥＥＥ１２１２レジスタ４４０７に、自分が映像送信機能を持つこと、およびパネル機能（制御画面機能）を持つことを記述しておき、これを中継ノード４１０２が読み込む（ステップＳ４６０１，Ｓ４７０４）。この送信ノード４１０１の機能を、中継ノード４１０２の機能として、代理して無線区間側のＩＥＥＥ１２１２相当機能（無線区間側のＣＳＲ空間）に反映し、無線ノード４１０３側には、上記映像送信機能、およびパネ

ル機能が中継ノード４１０２の機能であるものとして認識してもらう。この対応関係を、代理テーブル４２０８に図５４のように反映する（ステップＳ４７０５）。

【０１６５】

このようにして代理テーブル４２０８は、図５３／図５４のように構成される。また、送信ノード４１０１から見た中継ノード４１０２の内部構造を図５５に、無線ノード４１０３から見た中継ノード４１０２の内部構造を図５６に、それぞれ示す。

【０１６６】

なお、この時点で、ステップＳ４５０３の送信ノード構成情報の中に、送信ノード４１０１を制御するためのＨＡＶｉのバイトコードが含まれており、中継ノード４１０２は送信ノード４１０１の代理サーバ、すなわちＤＣＭ（デバイスコントロールモジュール）の機能を有していてもよい。この場合、このバイトコードは、中継ノード４１０２のＨＡＶｉ処理部４２１２内の仮想マシン上で稼働することになる。

【０１６７】

さて、中継ノード４１０２にパネル機能があるものと認識した無線ノード４１０３は、中継ノード４１０２の（パネルサブユニット）に対して、パネルの表示要求のコマンドを送出する（ステップＳ４５０５，Ｓ４８０２）。これを受信（ステップＳ４７０６）した中継ノード４１０２は、代理テーブル４２０８を参照し、このパネル機能の実体が送信ノード４１０１に存在していることを認識し、前記パネル表示要求コマンドを送信ノード４１０１に対してフォワードする（ステップＳ４５０６，Ｓ４７０７）。

【０１６８】

これを受信（ステップＳ４６０１）した送信ノード４１０１は、ＡＶ／Ｃプロトコルにてパネル応答（つまり、制御画面の送信）を行う。送信先は、中継ノード４１０２である（ステップＳ４６０３，Ｓ４５０７）。これを受信（ステップＳ４７０８）した中継ノード４１０２は、代理テーブル４２０８を参照して、これを無線ノード４１０３にフォワードする（ステップＳ４７０９，Ｓ４５０８，

Ｓ４８０３）。

【０１６９】

ここで、図５７に、無線ノード４１０３に送られてきた制御画面の一例を示す。この制御画面（パネル）では、６つの映画のタイトルを表示したボタンが提供される。これらのボタンは、例えば「ボタン１」、「ボタン２」、…等の名前が付けられており、ユーザがあるボタンを押すと、例えば「ボタン１が押されました」というコマンドの形で、パネルの送信元に送られる仕組みとなっているものとする。

【０１７０】

さて、無線ノード４１０３は、中継ノード４１０２が提供していると認識している映像送信サービスを受けようと考え（実際に提供しているのは送信ノード４１０１）、無線ノード制御パケットを使って（ステップＳ４５０９）、映像を流すための無線同期チャネル＃ｙを確保し、このチャネルを中継ノード４１０２の映像送信サブユニットに接続するためのコマンドを中継ノード４１０２に対して発行する（ステップＳ４８０４）。これを受信した中継ノード４１０２は、代理テーブル４２０８を参照して、実際にこのＡＶ／Ｃコマンドが発行されるべきノード（送信ノード４１９１）を確認し、ＩＥＥＥ１３９４バス上に必要な帯域を確保するとともに（同期チャネル＃ｘ）、内部のＩＳＯ信号送受信部４２０４を設定して、ＩＥＥＥ１３９４バスの同期チャネル＃ｘと無線同期チャネル＃ｙとを相互に接続する（ステップＳ４７１０，Ｓ４７１１，Ｓ４７１２，Ｓ４５１０）。また、中継ノード４１０２は、送信ノード４１０１に対し、同期チャネル＃ｘを映像送信サブユニットに接続するコマンドを発行する（ステップＳ４５１１，Ｓ４７１３）。これを受信（ステップＳ４６０４）した送信ノード４１０１は、映像送信サブユニットの実体である内部の映像ストリームの流れるパス（図４１で２重矢印になっている部分）をＩＥＥＥ１３９４バスの同期チャネル＃ｘに接続する。

【０１７１】

これと前後して、無線ノード４１０３のユーザは、見たい映像を選択するために図５７のパネルの中から適当な番組を選択すべく、制御画面のボタンを押す（

例えば、マウスを使ってクリックする、ペン入力する、タッチする、など）。この操作は、中継ノード４１０２に伝達され、これは代理テーブル４２０８の参照を経て送信ノード４１０１へのコマンドに変換される（ステップＳ４８０５，Ｓ４７１４，Ｓ４７１５，Ｓ４６０５，Ｓ４５１２，Ｓ４５１３）。

【０１７２】

この後、送信ノード４１０１は、同期チャネル＃ｘを通して、暗号化されたＭＰＥＧ映像を転送する（ステップＳ４５１４，Ｓ４６０６）。これは、中継ノード４１０２にて中継され、無線ノード４１０３に到達する（ステップＳ４７１６）。

【０１７３】

後の手続きは、第１の実施形態の場合と同様であり、暗号化されたＭＰＥＧ映像が無線ノード４１０３に到達する（ステップＳ４８０６）が、この時点で無線ノード４１０３はこの暗号を解くための鍵を有していないため、ＭＰＥＧ映像の送信元と認証手続きを開始する。認証手続き以降の手続きについては第１の実施形態と同様であるので、ここでの詳細な説明は省略する。

【０１７４】

なお、第１の実施形態に従えば、認証は送信ノード４１０１の映像送信サブユニットに相当する機能と、無線ノードの映像受信サブユニットに相当する機能との間で行われると考えられるが、第３の実施形態の場合には、このような認証方式の他に、送信ノード４１０１のパネルサブユニットが認証の対象となるような方式も考えられる。この場合は、送信ノード４１０１のパネルにデバイスＩＤが割り当てられることになる。

【０１７５】

なお、ＨＡＶｉにおいては、送信ノード４１０１から送られてくるバイトコードであるＤＣＭ等の中に、送信ノード４１０１を制御するための制御画面情報が含まれる場合がある。このようなモジュールをＤＤＩ（データドリブンインタラクション）と呼ぶ。このようなモジュールは、例えば中継ノード４１０２内のＨＡＶｉ処理部４２１２にて展開され、制御画面が生成される。本実施形態では、この制御画面（あるいは、それと同等の機能を持つ制御画面）を無線ノード側に

見せることを考える必要があるが、この場合は、代理サブユニット構成部４２０７が、このＤＤＩに含まれる画面構成情報を認識して（例えば、画面構成のためのシステムコールをイベントして認知して、生成される最終画面の概要を推察する方法や、完成した制御画面をもとにする方法等が考えられる）、パネルとしてこの制御画面を再構成し、無線区間に「パネルサブユニット」としてこれを公開する方法が考えられる。この場合には、代理テーブル４２０８には、このパネルと、ＤＤＩで生成されるべきＨＡＶｉやＡＶ／Ｃのコマンド（中継ノード４１０２から送信ノード４１０１に対して発行される）の対応テーブルが用意されることになる。この方法は、無線ノード４１０３内にＨＡＶｉバイトコードの仮想マシンが存在しなくても有効であるため、ＨＡＶｉ仮想マシンを持たない無線ノード４１０３から、ＨＡＶｉ機器の制御を可能とする方法である。

【０１７６】

（第４の実施形態）

次に、第４の実施形態について説明する。

【０１７７】

図５８に、本実施形態の全体構成の一例を示す。

【０１７８】

図５８に示されるように、第４の実施形態では、ある家庭のホームネットワークであるＩＥＥＥ１３９４バス６１０４と、公衆網（ここでは、一例としてインターネットとするが、電話網等でもよい）６１０５とが、ホームゲートウェイ６１０２で接続され、送信ノード６１０１と受信ノード６１０３との間で、認証手続き、暗号化の手続きを経た上で例えば映像データのやり取りを行う。ここで、インターネット６１０５（のアクセス網部分）は、ＩＥＥＥ１３９４バス６１０４と比べて通信帯域が非常に細く、ＩＥＥＥ１３９４バスでやり取りされる映像情報（一例としてＭＰＥＧ２映像であるとする）は、帯域が足りずに通せないため、ホームゲートウェイ６１０２においてトランスコーディング、つまりＭＰＥＧ２符号からＭＰＥＧ４符号への符号変換を行った上で、伝送を行うことを考える。

【０１７９】

第４の実施形態においても、第２の実施形態と同様に、ホームゲートウェイにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを終端する。すなわち、送信ノードとホームゲートウェイ、ホームゲートウェイト受信ノードとで、おのおのコピープロテクション手続きは閉じている。この実施形態においても、ホームゲートウェイは、送信ノードや受信ノードに対して代理サービスを提供し、また、コピープロテクションについては、ホームゲートウェイ自身が認証フォーマットを持ち、ホームゲートウェイ自身が１３９４バス区間および無線区間のＭＰＥＧデータの暗号化転送についてのそれぞれの責任を終端する。

【０１８０】

次に、図５９に、送信ノード６１０１の内部構造の一例を示す。これは基本的にはこれまでの実施形態と同様の構成である。

【０１８１】

次に、図６０に、ホームゲートウェイ６１０２の内部構造の一例を示す。

【０１８２】

ホームゲートウェイ６１０２の基本的な構成は、無線インタフェースではなくインターネットインタフェース６２０２を有している点、代理サブユニット構成部ではなく代理ホームページ作成部６２１０を有している点、ホームページの作成・蓄積部６２１１を有している点、暗号復号化部６２０４と暗号化部６２０５との間にＭＰＥＧ２／ＭＰＥＧ４変換部６２１４を有している点を除くと、第２の実施形態の中継ノードの構成とほぼ同様である。上記の相違点については順次説明していく。

【０１８３】

ホームゲートウェイ６１０２は、インターネット側のノードに対してＩＥＥＥ１３９４バス側のノード（本実施形態では、送信ノード２１０１）の代理サーバとなり、ＩＥＥＥ１３９４バス側のノードの機能を代理で提供する機能を持つ。送信ノード６１０１が提供しているサービス（本実施形態の場合、映像送信サービス）には、ホームゲートウェイ６１０２が提供しているホームページを介してアクセスすることが可能である。ここで、受信ノード６１０３からは、送信ノー

ド６１０１のサービスは、ホームゲートウェイ６１０２のホームページを介して見えるため、これをホームゲートウェイ６１０２が提供するＩＰ（インターネット）上のサービスとして解釈されてもよい。

【０１８４】

また、ホームゲートウェイ６１０２は、第２の実施形態と同様に、ＩＥＥＥ１３９４バス側から受信したデータ（ＭＰＥＧ２映像データ）をインターネット側にフォワードする機能を持つが、認証やデータの暗号化等、コピープロテクションに関する手続きがＩＥＥＥ１３９４バス区間とインターネット区間との両方について、このホームゲートウェイ６１０２において終端されている。ＩＥＥＥ１３９４バス側については、認証フォーマットＢｃｅｒｔをＩＥＥＥ１３９４コピープロテクション処理部６２０８に、インターネット区間側については、認証フォーマットＣｃｅｒｔをインターネット側コピープロテクション処理部６２１２にそれぞれ持ち、ＩＥＥＥ１３９４バスの同期チャネルから入力されてきた暗号化データについては、ＩＳＯ信号送受信部６２０３にて受信→暗号復号化部２２０４にて暗号復号化→復号化されたＭＰＥＧ２映像をＭＰＥＧ２／ＭＰＥＧ４変換部６２１４にてトランスコード→ＭＰＥＧ４映像を暗号化部６２０５にて再暗号化→ＡＶ信号送受信部６２０６にてインターネット側に送信、というプロセスを踏む。

【０１８５】

ここで、ＡｃｅｒｔとＢｃｅｒｔは、同じ認証機関（例えばＩＥＥＥ１３９４のコピープロテクションを担当する認証機関）が発行した認証フォーマットであると仮定するが、後述するインターネット区間の認証フォーマット（後述するＣｃｅｒｔとＤｃｅｒｔ）については、同じくこの認証機関が発行したものであってもよいし、インターネット区間を担当する別の認証機関が発行する認証フォーマットであってもよい。

【０１８６】

なお、本実施形態においては、認証フォーマット（Ａｃｅｒｔ～Ｄｃｅｒｔ）は、ノード（あるいはネットワークインタフェース）毎に１つ持つのではなく、サブユニット毎（サブユニット種別毎）、あるいはインターネットアプリケーシ

ョン毎に１つ持ってもよい。すなわち、異なるインターネットアプリケーションでは、異なる認証フォーマットを用いてもよい。ここで、フローとは、インターネットの（送信アドレス、送信ポート、受信アドレス、受信ポート）の組で表現される一連のデータ流を指す。

【０１８７】

次に、図６１に、受信ノード６１０３の内部構造の一例を示す。

【０１８８】

コピープロテクション処理部６３０３がインターネット向けの認証フォーマットＤｃｅｒｔを持っている。第２の実施形態との相違点は、インタフェース（インターネットインタフェース６３０１、制御パケット送受信部６３０２、ＡＶ信号送受信部６３０４）がインターネット対応となっている点である。ここで、制御パケット送受信部６３０２はＴＣＰ、ＡＶ信号送受信部６３９４はＵＤＰのトランスポートプロトコルを持つパケットの送受信モジュールであってもよい。

【０１８９】

次に、実際のコピープロテクションを施した上での映像送信全体のシーケンスについて、図６２／図６３（全体のシーケンス例）、図６４／図６５（送信ノード６１０３のフローチャート例）、図６６／図６７／図６８／図６９（ホームゲートウェイ６１０２のフローチャート例）、図７０／図７１（受信ノード６１０３のフローチャート例）を参照しながら説明する。

【０１９０】

まず、ホームゲートウェイ６１０２は、送信ノード６１０１のＩＥＥＥ１２１２レジスタの読み込みなどを通して、送信ノードについての属性や構成情報を収集する（ステップＳ６５０１，Ｓ６６０１，Ｓ６７０１，Ｓ６５０２，Ｓ６６０２，Ｓ６７０２）。これを通して、ホームゲートウェイ６１０２は、送信ノード６１０１が映像送信機能を持つこと、パネル機能を持つこと、認証フォーマットを持っていること等を把握する。

【０１９１】

これを受けて、ホームゲートウェイ６１０２は、送信ノード６１０１を遠隔制御するためのホームページを作成する（ステップＳ６５０３）。基本的には、送

信ノード６１０１が持つパネルと同様の画面を「送信ノード制御用ホームページ」として作成する。ホームページ上に配置された制御用のボタン等は、それぞれ送信ノード６１０１のパネルサブユニットのボタンに対応する等して、代理ホームページ作成部６２１０内の変換テーブルに対応の一覧が記述される。例えば、送信ノード６１０１のパネルサブユニットに「再生」とかかれているボタンが存在する場合には、該ホームページにも「再生」とかかれているボタンを用意して、この関係を前記変換テーブルに記述しておく。もし、このホームページのユーザがこのボタンを押した場合には、ホームゲートウェイ６１０２から送信ノード６１０１のパネルサブユニットの「再生」ボタンに対して「ボタンが押された」というインタラクションが返る形となる。図７２（ａ）に送信ノード６１０１のパネルサブユニットの持つパネルの一例を、図７２（ｂ）にホームゲートウェイ６１０２の作成した送信ノード制御用ホームページの一例をそれぞれ示す。

【０１９２】

さて、インターネット上の受信ノード６１０３は、インターネットを介してこのホームゲートウェイ６２０１にアクセスし、送信ノード６１０１の制御画面を含むホームページを要求し、このホームページが送付される（ステップＳ６５０４，Ｓ６８０１，Ｓ６７０３）。これを見て、受信ノード６１０３のユーザは、画面上の映像送信を要求するボタン（例えば、図７２（ｂ）の「再生」ボタン）を押したものとする。この結果、例えば「再生ボタンが押された」、というインタラクションが、インターネット経由でホームゲートウェイにＨＴＴＰを通じて通知される（ステップＳ６５０５，Ｓ６８０２，Ｓ６７０４）。

【０１９３】

この通知と前後して、ホームゲートウエイ６１０２と受信ノード６１０３との間で、やり取りされるストリームが転送されるＩＰフロー、すなわち（送信ＩＰアドレス、送信ポート、受信ＩＰアドレス、受信ポート）の組の決定や、セッション制御（符号化方式や認証方式等）のネゴシエーション等が行なわれる（ステップＳ６５０５，Ｓ６７０５，Ｓ６８０３）。例えば、ＲＴＳＰ（リアルタイムトランスポートストリーミングプロトコル）やＳＤＰ（セッションデスクリプションプロトコル）等を用いて、符号化方式や認証の方式、ポートの番号の決定な

どが行われる。

【０１９４】

ホームゲートウエイ６１０２は、これらの処理を受け、映像送信を行なう実体は、送信ノード６１０１の映像送信サブユニットであることを認識し、送信ノード６１０１に対してＡＶ／Ｃプロトコル等で、データ転送のための同期チャネル＃ｘの設定や、映像送信サブユニットに対して、映像送信の要求などのコマンドを発行する（ステップＳ６５０６）。

【０１９５】

これを受けて、送信ノード６１０１から同期チャネル＃ｘを通して、暗号化されたＭＰＥＧ映像がホームゲートウエイ６１０２に対して送出される（ステップＳ６５０７，Ｓ６６０３，Ｓ６６０４）。その後は、第２の実施形態のＩＥＥＥ１３９４側の手順と同様の手順で、認証先問合せ／応答、認証要求、認証・鍵交換手続き、交換鍵／シード転送等が行われ、ホームゲートウエイ６１０２にてコンテンツ鍵Ｋ１の計算ができるようになる（ステップＳ６５０８～Ｓ６５１４，Ｓ６６０５～Ｓ６６１１，Ｓ６７０６～Ｓ６７１５）。

【０１９６】

以降、同期チャネル＃ｘを通して暗号化されたＭＰＥＧ映像（ステップＳ６５１５，Ｓ６６１２，Ｓ６６１３）を受信したホームゲートウエイ６１０２は、暗号復号化部６２０４にて、これをコンテンツ鍵Ｋ１を用いてＭＰＥＧ２映像に復号化する（ステップＳ６５１６，Ｓ６５１７，Ｓ６７１６）。次に、抽出したＭＰＥＧ２映像を、ＭＰＥＧ２／ＭＰＥＧ４変換部６２１４でＭＰＥＧ４映像にトランスコードする（ステップＳ６５１８）。このＭＰＥＧ４映像を、コンテンツ鍵Ｋ２を用いて、暗号化部６２０５で再暗号化し（ステップＳ６５１９，Ｓ６５２０，Ｓ６７１７，Ｓ６７１８）、これをＩＰパケット化する。その場合、先のセッション制御の手順で決めたように、送信ＩＰアドレスはＣ（ホームゲートウエイのＩＰアドレス）、送信ポート番号はｃ、受信ＩＰアドレスはＤ（受信ノードのＩＰアドレス）、受信ポート番号はｄであるようなＩＰパケットを生成する（ステップＳ６５２１，Ｓ６７１９）。

【０１９７】

これを受信した受信ノード６１０３は、受信したデータが暗号化されていることを認識する（ステップＳ６８０４）。受信ノード６１０３は、このデータを送信しているのは、到着したパケットのＩＰヘッダを参照すること等により、ホームゲートウエイ６１０２であることを認識し、ホームゲートウエイ６１０２に対して、認証要求を送信する（ステップＳ６５２２，Ｓ６８０５）。この認証要求のパケットもＩＰパケットでもよい。認証要求のためのポート番号は、認証を行なう手続きに予め割当てられている番号を用いてもよい。この際、この認証要求のパケットに、ストリーム転送のフローＩＤ（Ｃ、ｃ、Ｄ、ｄ）を付与して転送する。このことにより、ホームゲートウエイ６１０２は、どのフローに対する認証要求であるかを認識することができる。図示はしていないが、この認証要求には、受信ノードの（本ストリーム用の）認証フォーマット等も含まれている。

【０１９８】

また、トランスポートプロトコルとしてＲＴＰ（Ｒｅａｌｔｉｍｅ　Ｔｒａｎｓｐｏｒｔ　Ｐｒｏｔｏｃｏｌ）を用いていること等を同時に伝えてもよい。

【０１９９】

これを受けてホームゲートウエイ６１０２は、フロー（Ｃ、ｃ、Ｄ、ｄ）のための認証要求であることを認識し、このフローのための認証フォーマットを含んだ認証要求を、受信ノード宛てに送り返す（ステップＳ６５２３，Ｓ６７２０～Ｓ６７２２，Ｓ６８０６，Ｓ６８０７）。このとき、この認証要求には前記フローＩＤ等が含まれる。

【０２００】

次に、両者は、認証・鍵交換手続き、交換鍵／シードの転送等を、ＩＰパケット上で行う（ステップＳ６５２４～Ｓ６５２６，Ｓ６７２３，Ｓ６７２４，Ｓ６８０８～Ｓ６８１０）。これにより、受信ノード６１０３は、コンテンツ鍵Ｋ２の生成が行なえるようになっている。

【０２０１】

よって、以降、コンテンツ鍵Ｋ２にて暗号化された、フロー（Ｃ、ｃ、Ｄ、ｄ）を通して送られてくるＭＰＥＧ４データ（ステップＳ６５２７～Ｓ６５３３，Ｓ６７２５，Ｓ６７２６，Ｓ６８１１）は、上記のように用意されたコンテンツ

鍵ｋ２にて復号化することが可能となる（ステップＳ６５３４）。復号化されたＭＰＥＧ４データは、ＭＰＥＧデコード部６３０６にて復号化され（ステップＳ６８１２）、これをディスプレイ部６３０７にて再生する（ステップＳ６８１３）。

【０２０２】

このように、家庭網とインターネットが相互接続された環境においても、代理機能を提供するホームゲートウェイと送信ノード、およびホームゲートウェイと受信ノードが認証手続きや鍵交換手続きを行うことで、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。このように、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【０２０３】

第２の実施形態と同様に、ホームゲートウェイ６１０２において、「生のＭＰＥＧデータ」が流れる部分、具体的には暗号復号化部６２０４、ＭＰＥＧ２／ＭＰＥＧ４変換部６２１４、暗号化部６２０５との間は、データコピーがなされないようにするための工夫、例えば一体のＬＳＩに封止する等の対策を立てておいてもよい。

【０２０４】

（第５の実施形態）

次に、第５の実施形態について説明する。

【０２０５】

第４の実施形態が、公衆網（インターネット）を介して家庭網にアクセスし、コピープロテクションを考慮した上で家庭網上の端末とインターネット上の端末間でコンテンツをやり取りする場合であったのに対し、第５の実施形態は、公衆網を介して家庭網間でコンテンツをやり取りする場合である。

【０２０６】

図７３に、本実施形態の全体構成図を示す。

【０２０７】

図７３に示されるように、第５の実施形態では、２つの家庭網８１０５，８１０７が公衆網（ここでは、一例としてインターネットとするが、Ｂ－ＩＳＤＮ等でもよい）８１０６にて接続されている。第１の家庭網８１０５上の送信ノード８１０１から、コピープロテクションを考慮した形で、ＡＶコンテンツを第２の家庭網８１０７上の受信ノード８１０４に送信する。ここで、第４の実施形態では、公衆網部分の通信帯域が非常に細い場合の例を示したが、本実施形態では、公衆網の通信帯域は十分な容量を持つものとする。

【０２０８】

第５の実施形態においては、第１の実施形態の中継ノードと同様に、ホームゲートウェイ８１０２，８１０３にて、ＩＥＥＥ１３９４バス８１０５，８１０７上のサービスを公衆網側に代理サービスする。すなわち、インターネット上からは、インターネットのサービスとして、家庭網上の装置やサービス、コンテンツが見える。また、ホームゲートウェイ８１０２，８１０３は、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りについてはこれらをフォワードする。

【０２０９】

送信ノード８１０１や受信ノード８１０４は、基本的には第４の実施形態と同様の構成である。

【０２１０】

図７４に、ホームゲートウェイ８１０２，８１０３の内部構造の一例を示す。

【０２１１】

ホームゲートウェイ８１０２の基本的な構成は、コピープロテクションを終端しない点（これは、第１の実施形態の中継ノードと同様）、および暗号の符号化・復号化・符号変換を行わない点（これも、第１の実施形態の中継ノードと同様）を除き、第４の実施形態のホームゲートウェイの構成とほぼ同様である。

【０２１２】

図７５に、全体のシーケンスの一例を示す。

【０２１３】

ここでは、第２の家庭網８１０７のユーザが、ホームゲートウェイ８１０３の

制御画面を使って、送信ノード８１０１のコンテンツを、インターネット８１０６を介して受信ノード８１０４に配信させる場合を考える。

【０２１４】

まず、第４の実施形態と同様に、ステップＳ８３０１の構成認識と、ステップＳ８３０２の送信ノード制御用ホームページ作成が行われる。

【０２１５】

第２の家庭網８１０７のユーザは、ホームゲートウェイ８１０３を操作し、ホームゲートウェイ８１０２から送信ノード制御用のホームページ（制御画面）を持ってくる（ステップＳ８３０３）。また、例えば図７６に例示するような受信ノード８１０４の制御画面も同時に開く。そこで、図７６のように、送信ノード内のコンテンツ一覧から、適当なものを例えばドラッグアンドドロップするなどして、ホームゲートウェイ８１０３に映像配信を命令する（ステップＳ８３０４）。

【０２１６】

すると、第４の実施形態と同様に、映像送信要求がホームゲートウェイ８１０２に（インターネットコマンドとして）発行され（ステップＳ８３０５）、これがホームゲートウェイ８１０２にてＡＶ／Ｃプロトコルコマンドに翻訳され、送信ノード８１０１から受信ノード８１０４間の通信パス（ＩＥＥＥ１３９４バス８１０５上の同期チャネル＃ｘ、インターネット上のコネクション、ＩＥＥＥ１３９４バス上の同期チャネル＃ｙ）が設定される（ステップＳ８３０６，Ｓ８３０７）。この上を、暗号鍵Ｋで暗号化されたＭＰＥＧ２映像が配信される（ステップＳ８３０８～Ｓ８３１０）。

【０２１７】

第１の実施形態と同様に、これを受信した受信ノード８１０６は、送信元に認証要求を発行する（ステップＳ８３１１）。受信ノード８１０４は、この映像はホームゲートウェイ８１０３から配信されていると解釈しているため、この認証要求はホームゲートウェイ８１０３に対して行われる。

【０２１８】

ホームゲートウェイ８１０３は、第４の実施形態と同様に、内部の変換テーブ

ル８２１１を参照して、これをホームゲートウェイ８１０２にフォワードする。これは、ホームゲートウェイ８１０３は、映像の配信元がホームゲートウェイ８１０２であると解釈しているからである。このフォワードは、認証要求８３１１の中身を変えない形で、インターネットパケットで行われる（ステップＳ８３１２）。同様に、ホームゲートウェイ８１０２は、これを受信ノード８１０１にフォワードする（ステップＳ８３１３）。送信ノード８１０１は、これをホームゲートウェイ８１０１から発行された認証要求であると解釈する。

【０２１９】

これと同様の手順を双方向に組み、送信ノード８１０１と受信ノード８１０４間で認証手続きが行われる（ステップＳ８３１４）。この間、ホームゲートウェイは、この手続きのパケットを中身を変更せずにフォワードする。認証と並行して、鍵情報のやり取りを行い、受信ノード８１０４は鍵の入手を行い、結局、暗号化されたＭＰＥＧ２映像の復号化ができるようになる。

【０２２０】

しかして、送信ノード８１０１が送信するＭＰＥＧ映像を、コンテンツキーＫを使って暗号化し、これが１３９４バスの同期チェネル＃ｘ、ホームゲートウェイ８１０２、公衆網、ホームゲートウェイ８１０３、１３９４バスの同期チェネル＃ｙという経路を辿って、受信ノード８１０３に到達する（ステップＳ８３１５～Ｓ８３１７）。そして、受信ノード８１０３では、暗号化されたＭＰＥＧ映像は、暗号鍵Ｋを使って暗号復号化され、デコードされて、再生表示される。

【０２２１】

このように、家庭網とインターネットが相互接続された環境においても、代理機能を提供するホームゲートウェイを介して、送信ノードと受信ノードが認証手続きや鍵交換手続きを行うことで、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。このように、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【０２２２】

なお、第５の実施形態において、公衆網の通信帯域が十分に広くない場合には、両ホームゲートウェイにおいて第４の実施形態の符号化変換（例えば、ホームゲートウェイ８１０２ではＭＰＥＧ２／ＭＰＥＧ４変換、ホームゲートウェイ８１０３ではＭＰＥＧ４／ＭＰＥＧ２変換）を行うことによって、若干の圧縮損はあるものの、両家庭網間でコピープロテクションを考慮したデータ転送を行うことが可能になる。

【０２２３】

（第６の実施形態）

第１の実施形態においては、中継ノードがＩＥＥＥ１３９４バスと無線網との両方に接続され、ＩＥＥＥ１３９４バス上の送信ノードと無線網上の無線ノードとの間で暗号化された映像データのやり取りをする場合の、認証・鍵交換方式を説明した。第１の実施形態では、認証フォーマットの交換等に代表される実際の認証・鍵交換は、送信ノードと無線ノード間で直接行ない、中継ノードは、これらのデータを透過的に中継する形で、これを実現してきた。

【０２２４】

これに対し、第６の実施形態では、第２の実施形態のように、認証・鍵交換の単位を送信ノードと中継ノード間、および中継ノードと無線ノード間でそれぞれ行なう。ただし、第２の実施形態と異なり、中継ノードにてコンテンツデータの暗号の復号化、および再暗号化を行なう必要が無いような方法の説明を行なう。すなわち、第２の実施形態では、到着したデータについて、中継ノードにてＩＥＥＥ１３９４区間の暗号の復号化を行い、無線区間の暗号化を再度行なうといった手順を使っていたが、これに対し、第６の実施形態では、ＩＥＥＥ１３９４バス側から到着した暗号化データをそのまま無線網上に転送できるような方法である。

【０２２５】

図７７に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第２の実施形態と同様である。

【０２２６】

図７８に、送信ノード９１０１の内部構造の一例を示す。これも第２の実施形

態と基本的には同様である。認証フォーマットＡｃｅｒｔが、ノードに一つ用意されている。

【０２２７】

図７９に、中継ノード９１０２の内部構造の一例を示す。認証フォーマットＢｃｅｒｔ、Ｃｃｅｒｔが、ネットワークインタフェース毎に一つ（ＩＥＥＥ１３９４側にＢｃｅｒｔ、無線網側にＣｃｅｒｔ）用意されている。ＩＥＥＥ１３９４側のＩＳＯ信号送受信部９２０３と無線ＩＳＯ信号送受信部９２０６間で、（復号化／再暗号化のプロセスを経ずに）直接暗号化されたストリーム信号がやり取りされる点を除いて、第２の実施形態と同様である。

【０２２８】

図８０に、無線ノード９１０３の内部構造の一例を示す。これも第２の実施形態と基本的には同様である。認証フォーマットＤｃｅｒｔが、ノードに一つ用意されている。

【０２２９】

これまでの実施形態と同様に、中継ノードでは、ＩＥＥＥ１３９４側には無線網上のサービスの、無線網側にはＩＥＥＥ１３９４上のサービスのそれぞれ代理サービス機能があるものとする。なお、ここでの詳細な説明は省略する。

【０２３０】

次に、本実施形態の全体のシーケンス例を図８１に示す。これまでの実施形態と同様に、例えば中継ノードが、送信ノードが提供しているサービス（映像送信サブユニット）を代理で無線網側に広告しており、無線ノード（の映像デコードサブユニット）が、中継ノードの代理機能に対してサービス（ＭＰＥＧ映像転送要求）を要求、中継ノードが実際のサービスを提供している送信ノードの映像送信サブユニットに対して、実際の映像転送要求を行う。実際の映像データは、暗号化された形でＩＥＥＥ１３９４上は同期チャネル＃ｘ上を、無線網上は無線同期チャネル＃ｙ上を転送されるものとする。なお、詳細はこれまでの実施形態と同様であるので、ここでの詳細な説明は省略する。

【０２３１】

また、送信ノード９１０１の動作手順例を図８２に、中継ノード９１０２の動

作手順例を図８３／図８４に、無線ノード９１０３の動作手順例を図８５／図８６に、それぞれ示す。

【０２３２】

本実施形態では、ＩＥＥＥ１３９４上の著作権保護方式である「５Ｃ　Ｄｉｇｉｔａｌ　ＴｒａｎｓｍｉｓｓｉｏｎＣｏｎｔｅｎｔ　Ｐｒｏｔｏｃｔｉｏｎ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ」の認証・鍵交換方式に基本的に準ずる手順を踏むものとする。なお、本実施形態では、認証・鍵交換方式をノード単位で行う場合について説明する（サブユニット単位で行う場合については、第７の実施形態で説明する）。

【０２３３】

さて、送信ノード９１０１は、ＩＥＥＥ１３９４の同期チャネル＃ｘ上に、コンテンツ鍵Ｋで暗号化されたＭＰＥＧ映像を転送する（ステップＳ８５０１，Ｓ８６０１，Ｓ８７０１）。これを受信した中継ノード９１０２は、このまま（受信したＭＰＥＧ映像を、コンテンツ鍵Ｋで暗号化されたまま）無線網側の無線同期チャネル＃ｙに対して転送する（ステップＳ８５０９，Ｓ８７０１）。

【０２３４】

同期チャネル＃ｙを通して受信したデータが暗号化されていると認識した中継ノード９１０２は、到着したデータのＣＩＰヘッダの送信ノードＩＤフィールド（ＳＩＤフィールド）を参照する等して、送信ノード９１０１と認証・鍵交換すべきであると認識する（ステップＳ８８０１）。中継ノード９１０２の認証フォーマットＢｃｅｒｔを含んだ認証要求パケットを送信ノード９１０１に対して転送する（ステップＳ８５０２，Ｓ８７０２）。

【０２３５】

これを受信した送信ノード９１０１は、送信ノードの認証フォーマットＡｃｅｒｔを含んだ認証要求パケットを中継ノード９１０２に対して送信する（ステップＳ８５０３，Ｓ８６０２，Ｓ８６０３，Ｓ８７０３）。

【０２３６】

次に、認証・鍵交換手続きを行って、送信ノード９１０１と中継ノード９１０２の両者で、認証鍵Ｋａｕｔｈ１を秘密裏に共有する（ステップＳ８５０４，Ｓ

８５０５，Ｓ８６０４，Ｓ８７０４）。

【０２３７】

ＩＥＥＥ１３９４著作権保護方式では、コンテンツ鍵Ｋは、交換鍵Ｋｘ、シードＮｃ、暗号制御情報ＥＭＩの３つの変数の関数Ｊにて計算される。すなわち、Ｋ＝Ｊ（Ｋｘ，Ｎｃ、ＥＭＩ）である。ここでＥＭＩは転送される暗号化データには必ず付与される値である。よって、送信ノード９１０１は、受信側（中継ノード、本実施形態の場合は無線ノードも）に対して、交換鍵ＫｘとシードＮｃの値を通知する必要がある。

【０２３８】

そこで、送信ノード９１０１は、中継ノード９１０２との間で共有した認証鍵Ｋａｕｔｈ１を使って、既知の関数ｆを使って、ｆ（Ｋｘ，Ｋａｕｔｈ）の形で中継ノード９１０２に送信する（ステップＳ８５０６，Ｓ８６０５，Ｓ８７０８，Ｓ８７０９）。中継ノード９１０２は、この値から、Ｋｘの値を算出することができる。同様に、シードＮｃの値も、送信ノード９１０１から中継ノード９１０２に転送される（ステップＳ８５０７，Ｓ８６０６，Ｓ８７１０）。ここで、中継ノード９１０２は、暗号を復号するコンテンツ鍵Ｋを生成するのに必要なＫｘ，Ｎｃの値をこの時点で認識したことになる。

【０２３９】

さて、同様の手続きが中継ノード９１０２と無線ノード９１０３の間でも行われる（ステップＳ８５１０～Ｓ８５１３，Ｓ８７０５～Ｓ８７０７，Ｓ８８０２～Ｓ８８０４）。この手続きは、送信ノード９１０１と中継ノード９１０２との間の認証・鍵交換手続きと同様であるので、ここでの詳細な説明は省略する。ここで、無線網の無線同期チャネル＃ｙ上を転送される暗号化されたデータにも、送信元ノードである中継ノード９１０２を識別できるようなアドレス情報等が付与されていてもよい。

【０２４０】

さて、中継ノード９１０２と無線ノード９１０１とで認証鍵Ｋａｕｔｈ２が共有できたものとする。本実施形態では、中継ノード９１０２は、暗号化されたＭＰＥＧ映像を暗号の復号化をすることなく、そのまま無線網（の無線同期チャネ

ル＃ｙ）にフォワード処理を行ってしまうため、中継ノード９１０２は無線ノード９１０３に対して、ＩＥＥＥ１３９４区間と同じ交換鍵ＫｘとシードＮｃの値を通知する必要がある（逆に通知できれば、無線ノード９１０３は暗号の復号化が可能である。ただし、ＩＥＥＥ１３９４区間と無線網区間は、同じコンテンツ保護ポリシーで運営されているものとする）。そこで、中継ノード９１０２は、Ｓ８５０６、Ｓ８５０７で受信したデータより算出したＫｘ，Ｎｃのそれぞれの値を、同様に無線ノード９１０３に対して送信する（ステップＳ８５１４，Ｓ８５１５，Ｓ８７０９，Ｓ８７１１，Ｓ８８０５～Ｓ８８０７）。具体的には、Ｋｘの値は認証鍵Ｋａｕｔｈ２の値を使ってｆ（Ｋｘ，Ｋａｕｔｈ２）を計算して、無線ノード９１０３に送出し、Ｎｃの値はそのまま転送する。

【０２４１】

無線ノード９１０３では、このようにして、中継ノードと同じ手順を使ってＫｘ、Ｎｃの値を認識できるため、同様の関数Ｊを使ってコンテンツ鍵Ｋの値を算出することができる（ステップＳ８５１６）。

【０２４２】

よって、送信ノード９１０１から送られてくる、コンテンツ鍵Ｋで暗号化されたＭＰＥＧ映像は、中継ノード９１０２で暗号の復号化がなされず、そのままフォワードして無線ノード９１０３まで転送されてきた場合（ステップＳ８５０８，Ｓ８５１７，Ｓ８６０７，Ｓ８７１２，Ｓ８８０９）でも、先にＳ８５１６で計算したコンテンツ鍵Ｋの値を使って、暗号の復号化ができる（ステップＳ８５１８，Ｓ８８１０）。その後、ＭＰＥＧ映像のデコード、ディスプレイ表示等が行われる。

【０２４３】

なお、本実施形態では、無線網上では無線同期チャネルが定義されており、暗号化されたＭＰＥＧ映像はこの無線同期チャネル上を転送されてくるとして説明を行ってきたが、第２の実施形態のように、無線網上でのＱＯＳデータ転送がイーサネットと同様の無線フレームを転送する場合にも、同様の方法（Ｋｘ，Ｎｃの値を中継ノードから無線ノードにフォワードする）が適用可能である。

【０２４４】

逆に言うと、本実施形態のような方法により、中継ノード９１０２では暗号の復号化および再暗号化が不要になり、高速なパケット転送も可能になることから、低コストな中継ノードの構築が可能となる。

【０２４５】

なお、この場合、ＩＥＥＥ１３９４側に送信ノード９１０２とは別のノード（別ノード）が存在しており、この別ノードから中継ノード９１０２を経て、無線ノード９１０３に別のコンテンツ鍵で暗号化されたデータ（厳密には同じＥＭＩを持ったデータ）を送信することはできない。コンテンツ鍵は、基本的にデータの送信ノード９１０１が決定する仕組みとなっていることから、別ノードが別のコンテンツ鍵を選択する可能性は十分にある。しかし、中継ノード９１０２と無線ノード９１０３との間で、既にコンテンツ鍵Ｋが一意に定義されている。すなわち、中継ノード９１０２と無線ノード９１０３との間では、同じＥＭＩ値については、１つのコンテンツ鍵しか共有できない。よって、両ノード間では、高々１つのコンテンツ鍵しか使うことができないため、別ノードからの（別のコンテンツ鍵で暗号化された）データを受信しても、これを中継ノード９１０２から無線ノード９１０３に転送する際に、別のコンテンツ鍵を生成できないため、これを復号化できないことになる。

【０２４６】

よって、中継ノード９１０２は、既に暗号化データを送信しているノード（本実施形態の場合、無線ノード９１０３）に対して、別のコンテンツ鍵を使う必要のある暗号化データの送信要求があった場合（例えば、ＩＥＥＥ１３９４の別ノードの代理サービスに対するサービス要求があった場合等）は、これを拒否することにより、未然に上記矛盾を回避することが可能となる。また、中継ノード９１０２は、既に無線ノード９１０３に対して暗号化データの送信を行っている場合には、該無線ノード９１０３に対しては、他のサービス（サブユニット）は見せない（代理サービス提供自体を中断する、あるいは暗号化ストリーム転送を伴う代理サービスの提供を中断する、等）、というやり方でも、同様の効果が考えられる。

【０２４７】

（第７の実施形態）

第６の実施形態では、認証・鍵交換の単位を送信ノードと中継ノードとの間、および中継ノードと無線ノードとの間でそれぞれ行ない、中継ノードにて暗号の復号化、および再暗号化を行なう必要が無いような方法であった。

【０２４８】

これに対し、第７の実施形態では、中継ノードにて暗号の復号化、および再暗号化を行なう必要が無いのは同様であるが、無線網側での認証・鍵交換の単位が、第２の実施形態と同じくサブユニット単位にでき、同じノード間でも複数のコンテンツ鍵を持つことができるような場合である。本実施形態によれば、ＩＥＥＥ１３９４上の複数送信ノードからの暗号化データの同時受信が可能となる。

【０２４９】

図８７に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は、送信ノード（ＰとＱ）が２つある点以外、基本的には第６の実施形態と同様である。

【０２５０】

送信ノード９８０１，９８１１の内部構成は、第６の実施形態と同様である。

【０２５１】

中継ノード９８０２の内部構成は、ＩＥＥＥ１３９４側では認証・鍵交換の単位がノード間であり、無線網側では認証・鍵交換の単位がサブユニット間である点を除いて、第６の実施形態と同様である。

【０２５２】

無線ノード９８０３の内部構成は、認証・鍵交換の単位がサブユニット間である点を除いて、第６の実施形態と同様である。

【０２５３】

なお、送信ノード９８０１，９８１１、無線ノード９８０２の動作手順は基本的には第６の実施形態と同様である。また、１つの送信ノードに対して中継を行う場合の中継ノード９８０３の動作手順も基本的には第６の実施形態と同様である。

【０２５４】

これまでの実施形態と同様に、中継ノードでは、ＩＥＥＥ１３９４側には無線網上のサービスの、無線網側にはＩＥＥＥ１３９４上のサービスのそれぞれ代理サービス機能があるものとする。なお、ここでの詳細な説明は省略する。

【０２５５】

次に、複数の送信ノードに対して中継を行う場合の中継ノード９８０２の動作手順例を図８８に、本実施形態の全体のシーケンス例を図８９／図９０に示す。これまでの実施形態と同様に、例えば中継ノードが、送信ノードが提供しているサービス（映像送信サブユニット）を代理で無線網側に広告しており、無線ノード（の映像デコードサブユニット）が、中継ノードの代理機能に対してサービス（ＭＰＥＧ映像転送要求）を要求、中継ノードが実際のサービスを提供している送信ノードの映像送信サブユニットに対して、実際の映像転送要求を行う。実際の映像データは、暗号化された形でＩＥＥＥ１３９４上は同期チャネル＃ｘ上を、無線網上は無線同期チャネル＃ｙ上を転送されるものとする。詳細はこれまでの実施形態と同様であるので、ここでの詳細な説明は省略する。

【０２５６】

本実施形態でも、ＩＥＥＥ１３９４上の著作権保護方式である「５Ｃ　Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｏｃｔｉｏｎ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ」の認証・鍵交換方式に基本的に準ずる手順を踏むものとする。

【０２５７】

さて、送信ノードＰ（９８０１）は、ＩＥＥＥ１３９４の同期チャネル＃ｘ上に、コンテンツ鍵Ｋ１で暗号化されたＭＰＥＧ映像を転送する（ステップＳ９２０１，Ｓ９３０１）。第６の実施形態と同様に、コンテンツ鍵Ｋ１は、Ｋ１＝Ｊ（Ｋｘｐ，Ｎｃｐ，ＥＭＩ）にて計算されるものとする。これを受信した中継ノード９８０２は、このまま（受信したＭＰＥＧ映像を、コンテンツ鍵Ｋ１で暗号化されたまま）無線網側の無線同期チャネル＃ｙに対して転送する（ステップＳ９２０９，Ｓ９３０１）。

【０２５８】

中継ノード９８０２が送信ノードＰに対して認証要求をし、鍵交換などを行っ

て、交換鍵ＫｘｐとシードＮｃｐを獲得する手順（ステップＳ９２０２～Ｓ９２０７，Ｓ９３０２）は、第６の実施形態と同様であるので、ここでの詳細な説明は省略する。この時点で、中継ノード９８０２は暗号を復号するために必要なＫｘｐ，Ｎｃｐの値を認識したことになる。

【０２５９】

さて、同様の認証・鍵交換手続きが中継ノード９８０２と無線ノード９８０３の間でも行われる（ステップＳ９２１０～Ｓ９２１７，Ｓ９３０３）。この手続きは第２の実施形態の送信ノードと中継ノード間の認証・鍵交換手続きと同様であるので、ここでの詳細な説明は省略する。ただし、認証先問い合わせや認証先応答、あるいは認証要求にサブユニットのＩＤの他、チャネル番号、あるいは暗号化データの送受信を行うことになるプラグの識別子を搭載して、これを行ってもよい。中継ノード９８０２、あるいは無線ノード９８０３が、「どの暗号化データについての認証・鍵交換手続きか」ということが識別できるようになり、後述するように、異なる鍵の暗号化データについては、同一のノード間の認証・鍵交換であったとしても、異なる鍵を通知することが可能になる。

【０２６０】

なお、この際、認証要求にチャネル番号を含める場合は、ステップＳ９２１０の認証先問い合わせとステップＳ９２１１の認証先応答は不要となる。

【０２６１】

さて、中継ノード９８０２と無線ノード９８０３で認証鍵Ｋａｕｔｈ１が共有できたものとする。本実施形態でも、中継ノード９８０２は、暗号化されたＭＰＥＧ映像を暗号の復号化をすることなく、そのまま無線網（の無線同期チャネル＃ｙ）にフォワード処理を行ってしまうため、中継ノード９８０２は無線ノード９８０３に対して、交換鍵Ｋｘｐとシードの値を通知する必要がある（逆に通知できれば、無線ノード９８０３は暗号の復号化が可能である）。そこで、中継ノード９８０２は、Ｓ９２０６、Ｓ９２０７で受信したデータより算出したＫｘｐ，Ｎｃｐのそれぞれの値を、同様に無線ノード９８０３に対して送信する（ステップＳ９２１６，Ｓ９２１７）。Ｋｘｐの値は認証鍵Ｋａｕｔｈ１の値を使ってｆ（Ｋｘｐ，Ｋａｕｔｈ１）を計算して、無線ノード９８０３に送出する

（ステップＳ９２１６）。

【０２６２】

無線ノード９８０３では、このようにして、中継ノード９８０２と同じ手順を使ってＫｘｐ、Ｎｃｐの値を認識できるため、同様の関数Ｊを使ってコンテンツ鍵Ｋ１の値を算出することができる（ステップＳ９２１８）。

【０２６３】

よって、送信ノードＰから送られてくる、コンテンツ鍵Ｋ１で暗号化されたＭＰＥＧ映像は、中継ノード９８０２で暗号の復号化をせずに、そのままフォワードして無線ノード９８０３まで転送されてきた場合（ステップＳ９２０８，Ｓ９２１９）でも、先にステップＳ９２１８で計算したコンテンツ鍵Ｋ１の値を使って、暗号の復号化ができる（ステップＳ９２２０）。その後、ＭＰＥＧ映像のデコード、ディスプレイ表示等が行われる。

【０２６４】

本実施形態のような方法でも、中継ノード９８０２では暗号の復号化、および再暗号化が不要になり、高速なパケット転送も可能になることから、低コストな中継ノードの構築が可能となる。

【０２６５】

さて、次に、別の送信ノードＱ（９８１１）が、同時に中継ノード９８０２を介して無線ノード９８０３に対して別のコンテンツ鍵Ｋ２で暗号化されたデータを送信する場合（ステップＳ９２２１，Ｓ９２２９，Ｓ９３０４）を考える。

【０２６６】

本実施形態の前半と同様に、送信ノードＱと中継ノード９８０２との間で認証・鍵交換が行われ（ステップＳ９２２２～Ｓ９２２７）、中継ノード９８０２は交換鍵ＫｘｑとシードＮｃｑの値をそれぞれ得ることができる。

【０２６７】

本実施形態においては、中継ノード９８０２と無線ノード９８０３との間の認証は、サブユニット間単位であるので、暗号化データの送受が異なるサブユニット間で行われているものとすれば、中継ノード９８０２と無線ノード９８０３との間で複数の認証・鍵交換が可能となる。

【０２６８】

すなわち、本実施形態の前半と同様に、中継ノード９８０２と無線ノード９８０３との間で、本実施形態の前半とは異なるサブユニット間で認証・鍵交換を行っていく（ステップＳ９２３０～Ｓ９２３５，Ｓ９３０５）。その上で、中継ノード９８０２は、送信ノードＱと自ノード（中継ノード）９８０２との間の交換鍵ＫｘｑとシードＮｃｑを、無線ノード９８０３にフォワードする（ステップＳ９２３６，Ｓ９２３７，Ｓ９３０５，Ｓ９３０６）。

【０２６９】

無線ノード９８０３では、このようにして、Ｋｘｑ、Ｎｃｑの値を認識できるため、同様の関数Ｊを使ってコンテンツ鍵Ｋ２の値を算出することができる（ステップＳ９２３８）。

【０２７０】

よって、送信ノードＱから送られてくる、コンテンツ鍵Ｋ２で暗号化されたＭＰＥＧ映像は、中継ノード９８０２で暗号の復号化をせずに、そのままフォワードして無線ノード９８０３まで転送されてきた場合（ステップＳ９２２８，Ｓ９２２９）でも、先にステップＳ９２３８で計算したコンテンツ鍵Ｋ２の値を使って、暗号の復号化ができる（ステップＳ９２４０）。つまり、２つの異なるコンテンツ鍵（本実施形態ではＫ１とＫ２）で暗号化されたＭＰＥＧ映像の同時受信が可能となる。

【０２７１】

なお、第６の実施形態と第７の実施形態では、ＩＥＥＥ１３９４と無線網との相互接続を行う場合を例に説明してきたが、インターネット等のその他の網についても適用可能である。

【０２７２】

なお、第１～第７の実施形態において例示したデータ転送の方向とは逆の方向にデータ転送する場合（例えば、無線ノードからＩＥＥＥ１３９４上のノードへデータ転送する場合）にも、本発明は適用可能である。

【０２７３】

また、第１～第７の実施形態において、無線ノードやＩＥＥＥ１３９４上のノ

ードについては、コンテンツについて送信機能または受信機能の一方に着目して説明したが、無線ノードやＩＥＥＥ１３９４上のノードは、コンテンツについて送信機能と受信機能の両方を備えることも可能である。

【０２７４】

また、認証手続きや、鍵交換手続き（コンテンツ鍵共有手続き）は、これまでに例示したものに限定されず、他の種々の方法が用いられる場合にも本発明は適用可能である。

【０２７５】

また、以上では、家庭網ネットワークとして実施形態を説明したが、もちろん、本発明は家庭網以外のネットワークにも適用可能である。

【０２７６】

なお、以上の各機能は、ソフトウェアとしても実現可能である。

【０２７７】

また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【０２７８】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０２７９】

【発明の効果】

本発明によれば、同じネットワークでは接続されていない装置間で、保護すべきコンテンツの送受信のためのコンテンツ保護手続きを行うことが可能になる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態に係るネットワークの全体構成の一例を示す図

【図２】

送信ノードの内部構造の一例を示す図

【図３】

中継ノードの内部構造の一例を示す図

【図４】

無線ノードの内部構造の一例を示す図

【図５】

全体のシーケンスの一例を示す図

【図６】

全体のシーケンスの一例を示す図

【図７】

送信ノードの動作手順の一例を示すフローチャート

【図８】

送信ノードの動作手順の一例を示すフローチャート

【図９】

中継ノードの動作手順の一例を示すフローチャート

【図１０】

中継ノードの動作手順の一例を示すフローチャート

【図１１】

中継ノードの動作手順の一例を示すフローチャート

【図１２】

無線ノードの動作手順の一例を示すフローチャート

【図１３】

無線ノードの動作手順の一例を示すフローチャート

【図１４】

無線ノード構成情報パケットの一例を示す図

【図１５】

代理テーブルの一例を示す図

【図１６】

代理テーブルの一例を示す図

【図１７】

送信ノードから見た中継ノードの内部構造を説明するための図

【図１８】

無線ノードから見た中継ノードの内部構造を説明するための図

【図１９】

無線ノード制御パケットの一例を示す図

【図２０】

本発明の第２の実施形態に係るネットワークの全体構成の一例を示す図

【図２１】

送信ノードの内部構造の一例を示す図

【図２２】

中継ノードの内部構造の一例を示す図

【図２３】

無線ノードの内部構造の一例を示す図

【図２４】

全体のシーケンスの一例を示す図

【図２５】

全体のシーケンスの一例を示す図

【図２６】

送信ノードの動作手順の一例を示すフローチャート

【図２７】

送信ノードの動作手順の一例を示すフローチャート

【図２８】

中継ノードの動作手順の一例を示すフローチャート

【図２９】

中継ノードの動作手順の一例を示すフローチャート

【図３０】

中継ノードの動作手順の一例を示すフローチャート

【図３１】

中継ノードの動作手順の一例を示すフローチャート

【図３２】

無線ノードの動作手順の一例を示すフローチャート

【図３３】

無線ノードの動作手順の一例を示すフローチャート

【図３４】

代理テーブルの一例を示す図

【図３５】

代理テーブルの一例を示す図

【図３６】

送信ノードから見た中継ノードの内部構造を説明するための図

【図３７】

無線ノードから見た中継ノードの内部構造を説明するための図

【図３８】

無線フレームのフォーマットの一例を示す図

【図３９】

無線制御パケットのフォーマットの一例を示す図

【図４０】

本発明の第３の実施形態に係るネットワークの全体構成の一例を示す図

【図４１】

送信ノードの内部構造の一例を示す図

【図４２】

中継ノードの内部構造の一例を示す図

【図４３】

無線ノードの内部構造の一例を示す図

【図４４】

全体のシーケンスの一例を示す図

【図４５】

全体のシーケンスの一例を示す図

【図４６】

送信ノードの動作手順の一例を示すフローチャート

【図４７】

送信ノードの動作手順の一例を示すフローチャート

【図４８】

中継ノードの動作手順の一例を示すフローチャート

【図４９】

中継ノードの動作手順の一例を示すフローチャート

【図５０】

中継ノードの動作手順の一例を示すフローチャート

【図５１】

無線ノードの動作手順の一例を示すフローチャート

【図５２】

無線ノードの動作手順の一例を示すフローチャート

【図５３】

代理テーブルの一例を示す図

【図５４】

代理テーブルの一例を示す図

【図５５】

送信ノードから見た中継ノードの内部構造を説明するための図

【図５６】

無線ノードから見た中継ノードの内部構造を説明するための図

【図５７】

無線ノードに送られてきた制御画面の一例を示す図

【図５８】

本発明の第４の実施形態に係るネットワークの全体構成の一例を示す図

【図５９】

送信ノードの内部構造の一例を示す図

【図６０】

ホームゲートウェイの内部構造の一例を示す図

【図６１】

受信ノードの内部構造の一例を示す図

【図６２】

全体のシーケンスの一例を示す図

【図６３】

全体のシーケンスの一例を示す図

【図６４】

送信ノードの動作手順の一例を示すフローチャート

【図６５】

送信ノードの動作手順の一例を示すフローチャート

【図６６】

ホームゲートウェイの動作手順の一例を示すフローチャート

【図６７】

ホームゲートウェイの動作手順の一例を示すフローチャート

【図６８】

ホームゲートウェイの動作手順の一例を示すフローチャート

【図６９】

ホームゲートウェイの動作手順の一例を示すフローチャート

【図７０】

受信ノードの動作手順の一例を示すフローチャート

【図７１】

受信ノードの動作手順の一例を示すフローチャート

【図７２】

送信ノードのパネルとホームゲートウェイの送信ノード制御用ホームページの一例を示す図

【図７３】

本発明の第５の実施形態に係るネットワークの全体構成の一例を示す図

【図７４】

ホームゲートウェイの内部構造の一例を示す図

【図７５】

全体のシーケンスの一例を示す図

【図７６】

制御画面の一例を示す図

【図７７】

本発明の第６の実施形態に係るネットワークの全体構成の一例を示す図

【図７８】

送信ノードの内部構造の一例を示す図

【図７９】

中継ノードの内部構造の一例を示す図

【図８０】

無線ノードの内部構造の一例を示す図

【図８１】

全体のシーケンスの一例を示す図

【図８２】

送信ノードの動作手順の一例を示すフローチャート

【図８３】

中継ノードの動作手順の一例を示すフローチャート

【図８４】

中継ノードの動作手順の一例を示すフローチャート

【図８５】

無線ノードの動作手順の一例を示すフローチャート

【図８６】

無線ノードの動作手順の一例を示すフローチャート

【図８７】

本発明の第７の実施形態に係るネットワークの全体構成の一例を示す図

【図８８】

中継ノードの動作手順の一例を示すフローチャート

【図８９】

全体のシーケンスの一例を示す図

【図９０】

全体のシーケンスの一例を示す図

【符号の説明】

１０１，２１０１，４１０１，６１０１，８１０１，９１０１，９８０１，９８１１…送信ノード

１０２，２１０２，４１０２，９１０２，９８０２…中継ノード

１０３，２１０３，４１０３，６１０４，９１０３，９８０３…無線ノード

６１０２，８１０２，８１０３…ホームゲートウェイ

６１０３，８１０４…受信ノード

１０４，２１０４，４１０４，８１０５，８１０７，９１０４，９８０４…ＩＥＥＥ１３９４バス

６１０５，８１０６…公衆網

２０１，２２０１，４２０１，６２０１，８２０１，９１０１…ＩＥＥＥ１３９４インタフェース

２０２，２２０２，４２０２，９２０２…無線インタフェース

２０３，２２０７，４２０３，６２０７，８２０３，９２０７…ＡＶ／Ｃプロトコル処理部

２０４，２２０３，４２０４，６２０３，８２０４，９２０３…ＩＳＯ信号送受信部

２０５，２２０６，４２０５，９２０６…無線ＩＳＯ信号送受信部

２０６，２２０９，４２０６，６２０９，９２０９…１３９４バス構成認識部

２０７，２２１０，４２０７，８２０７，９２１０…代理サブユニット構成部

２０８，２２１４，４２０８，６２１５，９２１４…代理テーブル

２０９，２２１１，４２０９，９２１１…無線区間構成認識部

２１０，４２１０，８２０９…コピープロテクション制御／フォワード部

２２０８，６２０８…ＩＥＥＥ１３９４コピープロテクション処理部

２２１２，９２１２…無線区間コピープロテクション部

８２１１…変換テーブル

２１１，２２１３，４２１１，９２１３…無線ノード制御パケット送受信部

２２０４，６２０４…暗号復号化部

２２０５，６２０５…暗号化部

４２１２…ＨＡＶｉ処理部

４２１３…ＩＥＥＥ１２１２レジスタ

６２０６，８２０５…ＡＶ信号送受信部

６２０２，８２０２…インターネットインタフェース

６２１０，８２０８…代理ホームページ作成部

６２１１，８２１０…ホームページ作成・蓄積部

６２１２…インターネット側プロテクション処理部

６２１３…制御パケット送受信部

６２１４…ＭＰＥＧ２／ＭＰＥＧ４変換部

６２０６…制御パケット処理信部

３０１，２３０１，４３０１，９３０１…無線インタフェース

３０２，２３０２，４３０２，９３０２…無線ノード制御パケット送受信部

３０３，２３０３，４３０３，６３０３，９３０３…コピープロテクション処理部

３０４，２３０４，４３０４，９３０４…無線ＩＳＯ信号送受信部

３０５，２３０５，４３０５，６３０５，９３０５…暗号復号化部

３０６，２３０６，４３０６，６３０６，９３０６…ＭＰＥＧデコード部

３０７，２３０７，４３０７，６３０７，９３０７…ディスプレイ部

６３０１…インターネットインタフェース

６３０２…制御パケット送受信部

６３０４…ＡＶ信号送受信部

４０１，２４０１，４４０１，６４０１，９４０１…ＩＥＥＥ１３９４インタフェース

４０２，２４０２，４４０２，６４０２，９４０２…ＡＶ／Ｃプロトコル処理部

４０３，２４０３，４４０３，６４０３，９４０３…コピープロテクション処

理部

４０４，２４０４，４４０４，６４０４，９４０４…ＩＳＯ信号送受信部

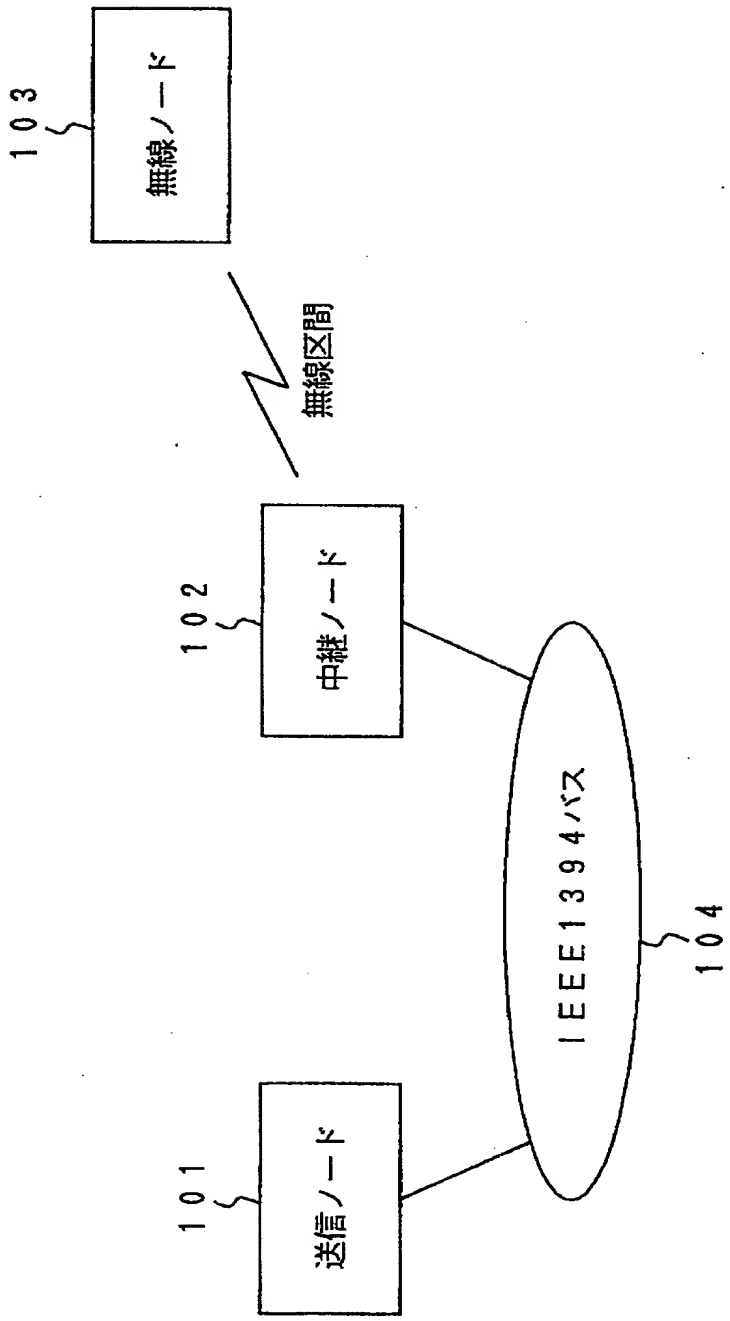
４０５，２４０５，４４０５，６４０５，９４０５…暗号化部

４０６，２４０６，４４０６，６４０６，９４０６…ＭＰＥＧストレージ部

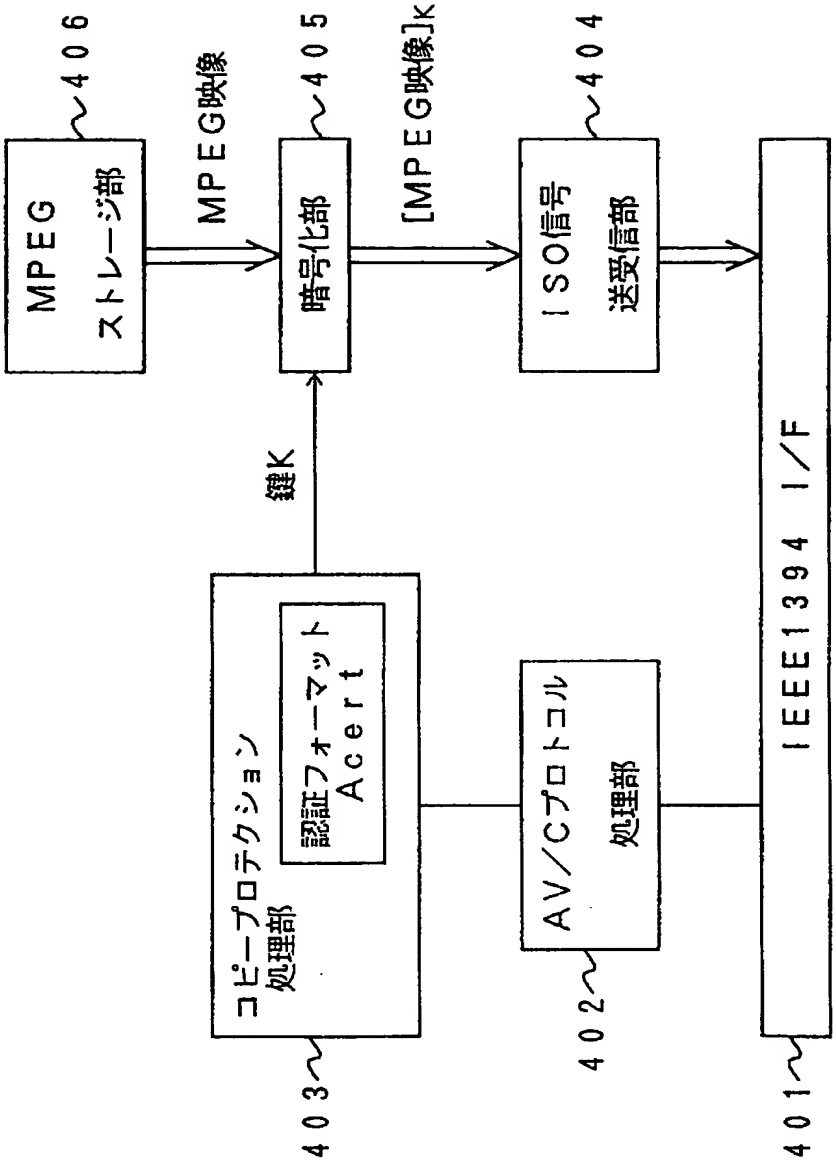
４４０７…ＩＥＥＥ１２１２レジスタ

【書類名】　　図面

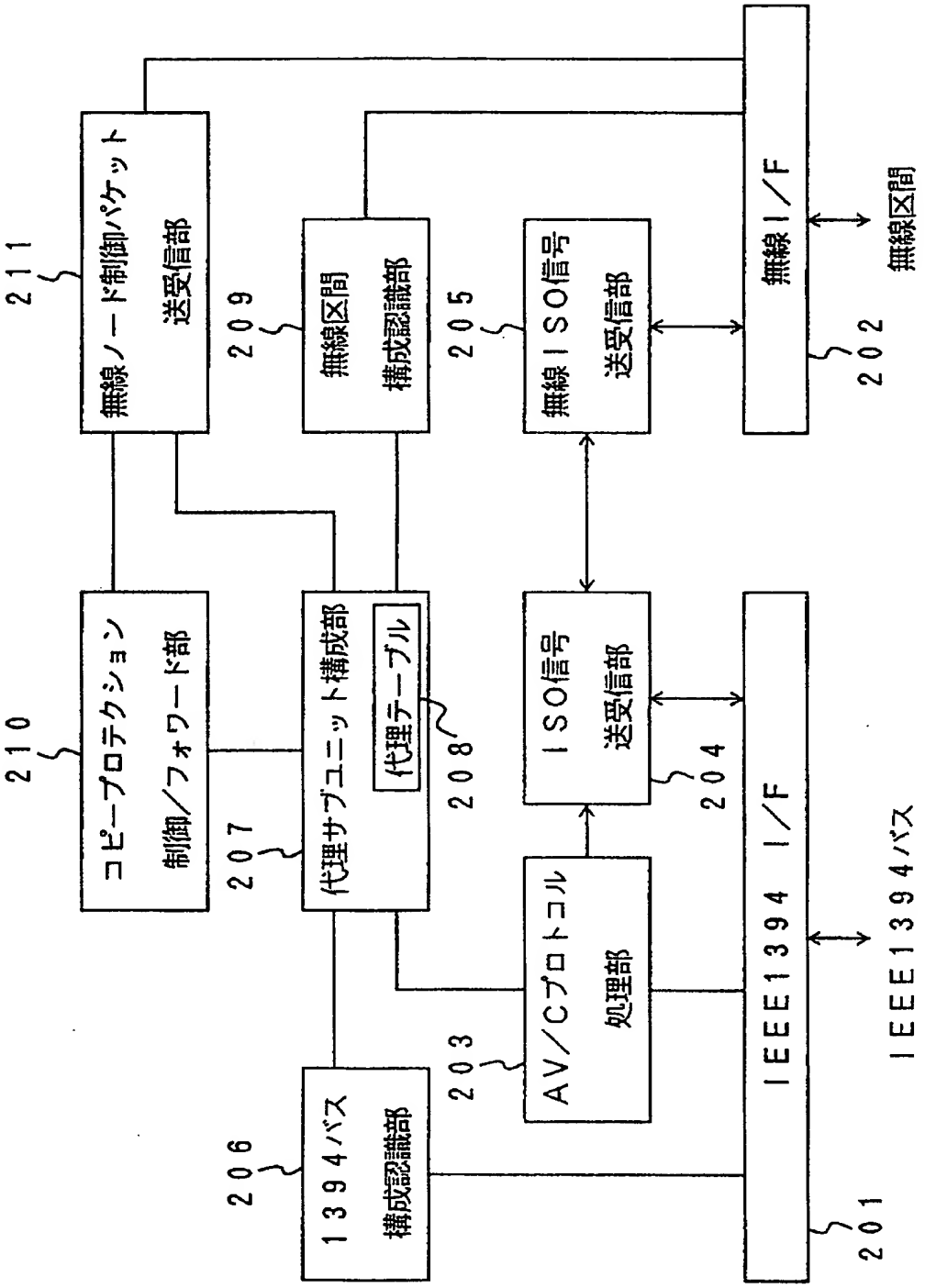
【図１】



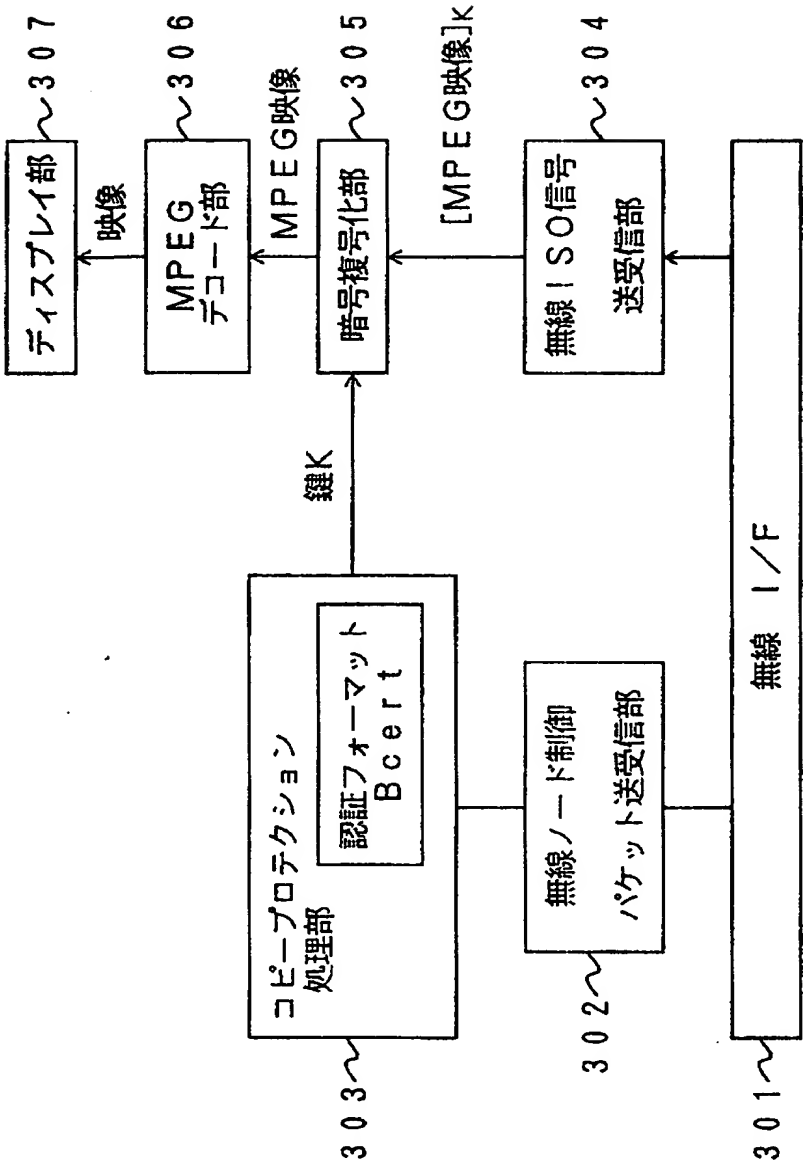
【図２】


MPEG
ストレージ部
406
MPEG映像
暗号化部
405
[MPEG映像]K
ISO信号
送受信部
404
鍵K
コピープロテクション
処理部
認証フォーマット
Acert
403
AV/Cプロトコル
処理部
402
IEEE1394 I/F
401

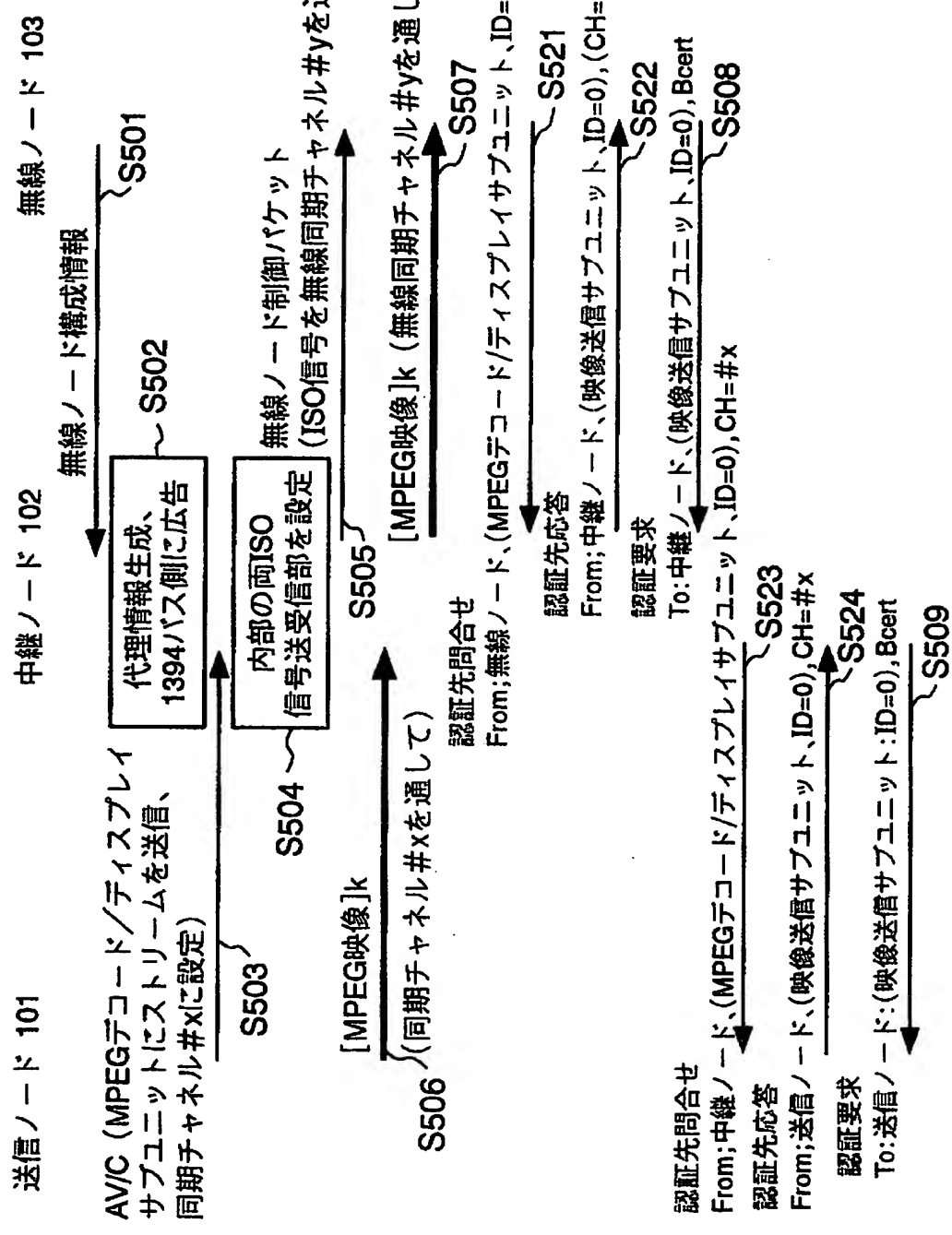
【図３】


無線ノード制御パケット
送受信部
211
無線区間
構成認識部
209
205
無線ＩＳＯ信号
送受信部
無線Ｉ／Ｆ
202
無線区間
コピープロテクション
制御／フォワード部
210
代理サブユニット構成部
207
代理テーブル
208
ＩＳＯ信号
送受信部
204
ＩＥＥＥ１３９４　Ｉ／Ｆ
ＩＥＥＥ１３９４バス
１３９４バス
構成認識部
206
203
ＡＶ／Ｃプロトコル
処理部
201

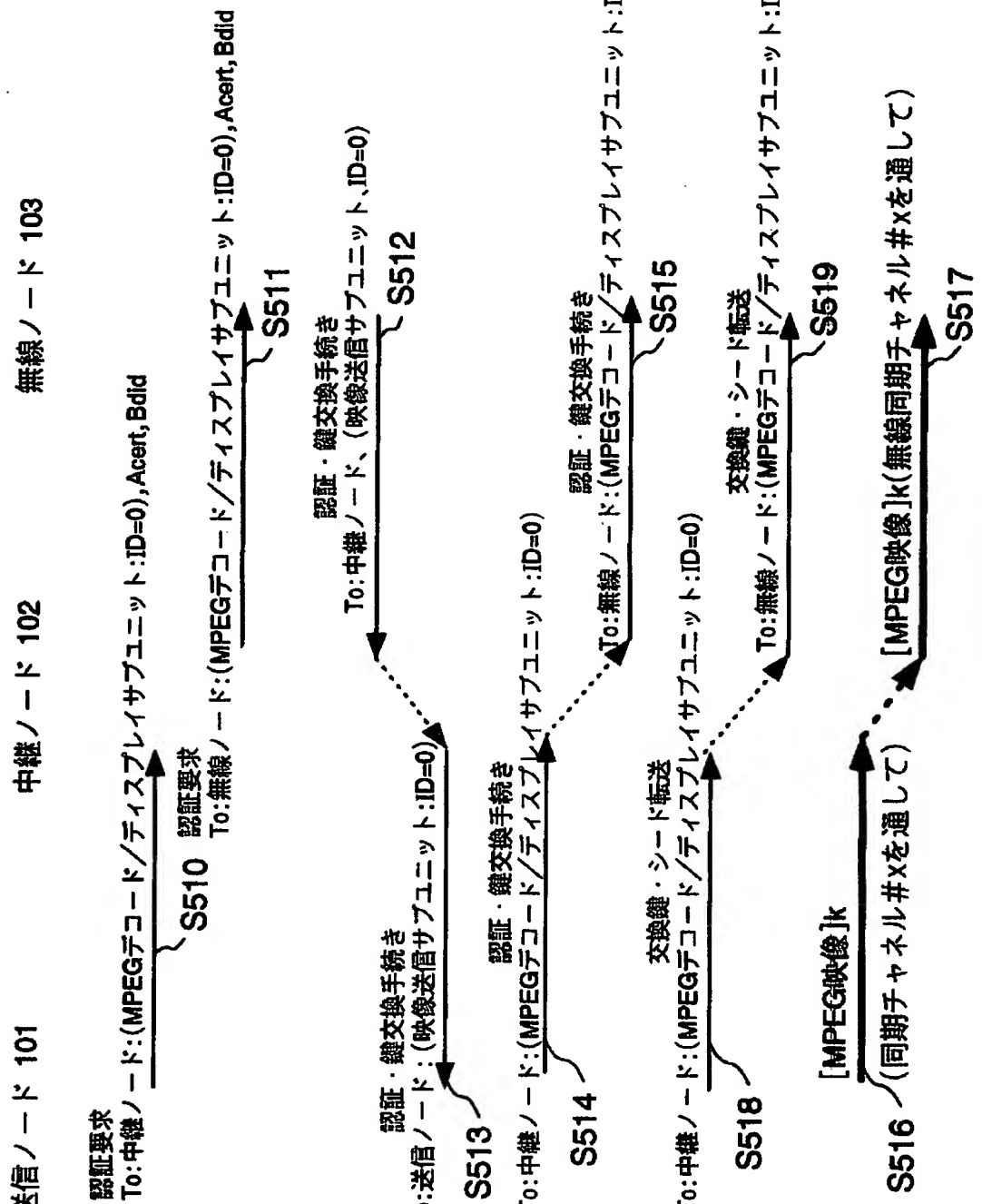
【図４】


ディスプレイ部
～３０７
映像
MPEG
デコード部
～３０６
MPEG映像
暗号複号化部
～３０５
[MPEG映像]K
無線ISO信号
送受信部
～３０４
鍵K
コピープロテクション
処理部
認証フォーマット
Bcert
～３０３
無線ノード制御
パケット送受信部
～３０２
無線 I/F
～３０１

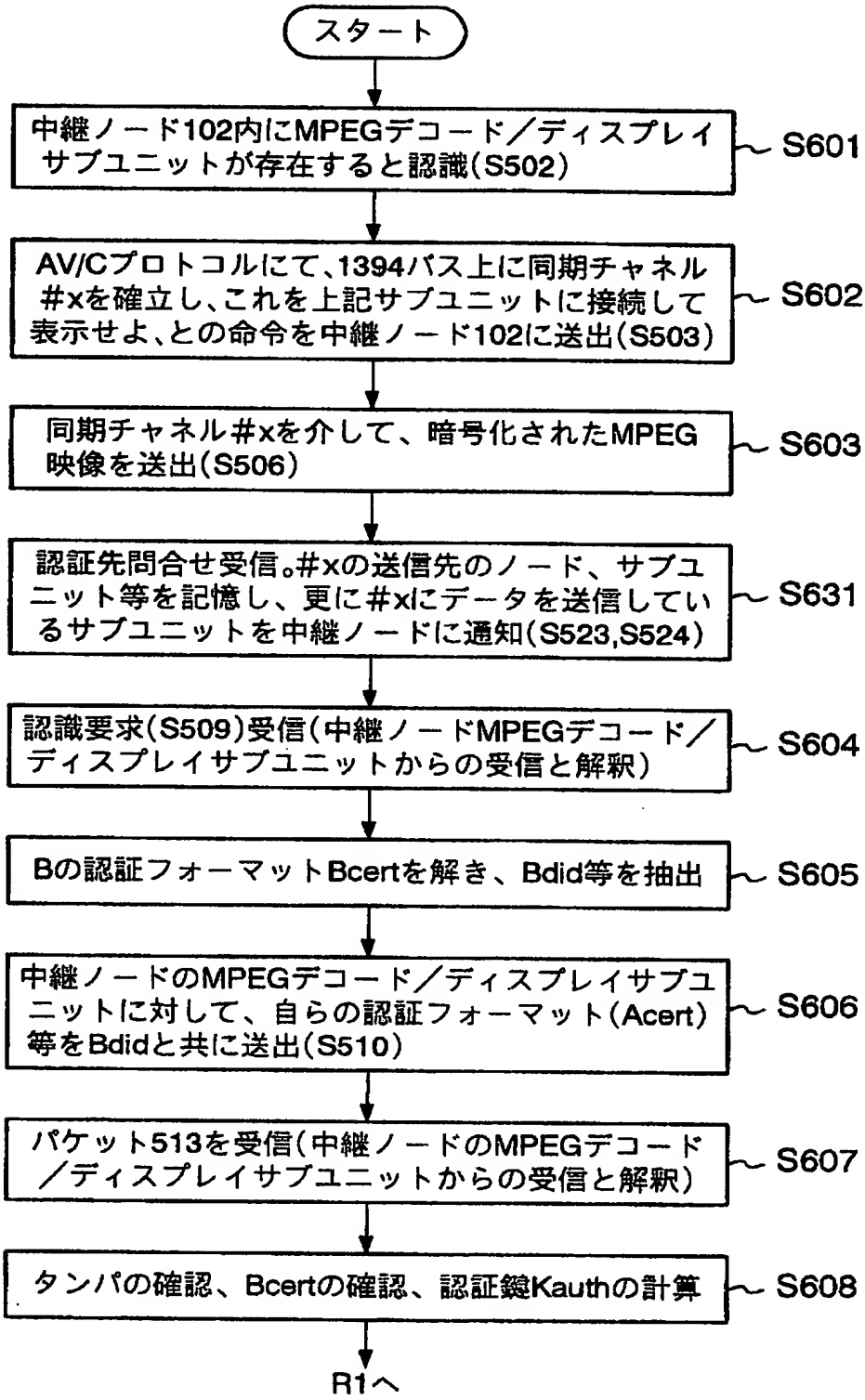
【図５】


送信ノード 101
中継ノード 102
無線ノード 103
無線ノード構成情報
S501
代理情報生成、
1394バス側に広告
S502
AV/C (MPEGデコード/ディスプレイ
サブユニットにストリームを送信、
同期チャネル#xに設定)
S503
内部の両ISO
信号送受信部を設定
S504
無線ノード制御パケット
(ISO信号を無線同期チャネル#yを通して送信)
S505
[MPEG映像]k
(同期チャネル#xを通して)
S506
[MPEG映像]k (無線同期チャネル#yを通して)
S507
認証先問合せ
From;無線ノード、(MPEGデコード/ディスプレイサブユニット、ID=0),(CH=#y)
S521
認証先応答
From;中継ノード、(映像送信サブユニット、ID=0),(CH=#y)
S522
認証要求
To:中継ノード、(映像送信サブユニット、ID=0),Bcert
S508
認証先問合せ
From;中継ノード、(MPEGデコード/ディスプレイサブユニット、ID=0),CH=#x
S523
認証先応答
From;送信ノード、(映像送信サブユニット、ID=0),CH=#x
S524
認証要求
To:送信ノード:(映像送信サブユニット:ID=0),Bcert
S509

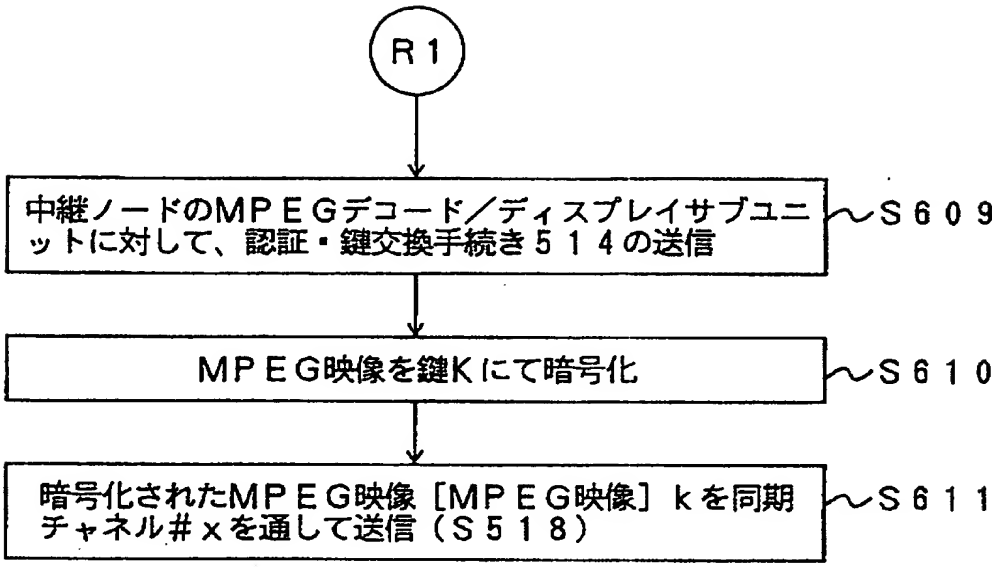
【図６】


送信ノード 101
中継ノード 102
無線ノード 103
認証要求
To:中継ノード:(MPEGデコード/ディスプレイサブユニット:ID=0),Acert,Bdid
S510
認証要求
To:無線ノード:(MPEGデコード/ディスプレイサブユニット:ID=0),Acert,Bdid
S511
認証・鍵交換手続き
To:中継ノード、(映像送信サブユニット、ID=0)
S512
認証・鍵交換手続き
To:送信ノード:(映像送信サブユニット:ID=0)
S513
認証・鍵交換手続き
To:中継ノード:(MPEGデコード/ディスプレイサブユニット:ID=0)
S514
認証・鍵交換手続き
To:無線ノード:(MPEGデコード/ディスプレイサブユニット:ID=0)
S515
交換鍵・シード転送
To:中継ノード:(MPEGデコード/ディスプレイサブユニット:ID=0)
S518
交換鍵・シード転送
To:無線ノード:(MPEGデコード/ディスプレイサブユニット:ID=0)
S519
[MPEG映像]k
S516
(同期チャネル#xを通して)
[MPEG映像]k(無線同期チャネル#xを通して)
S517

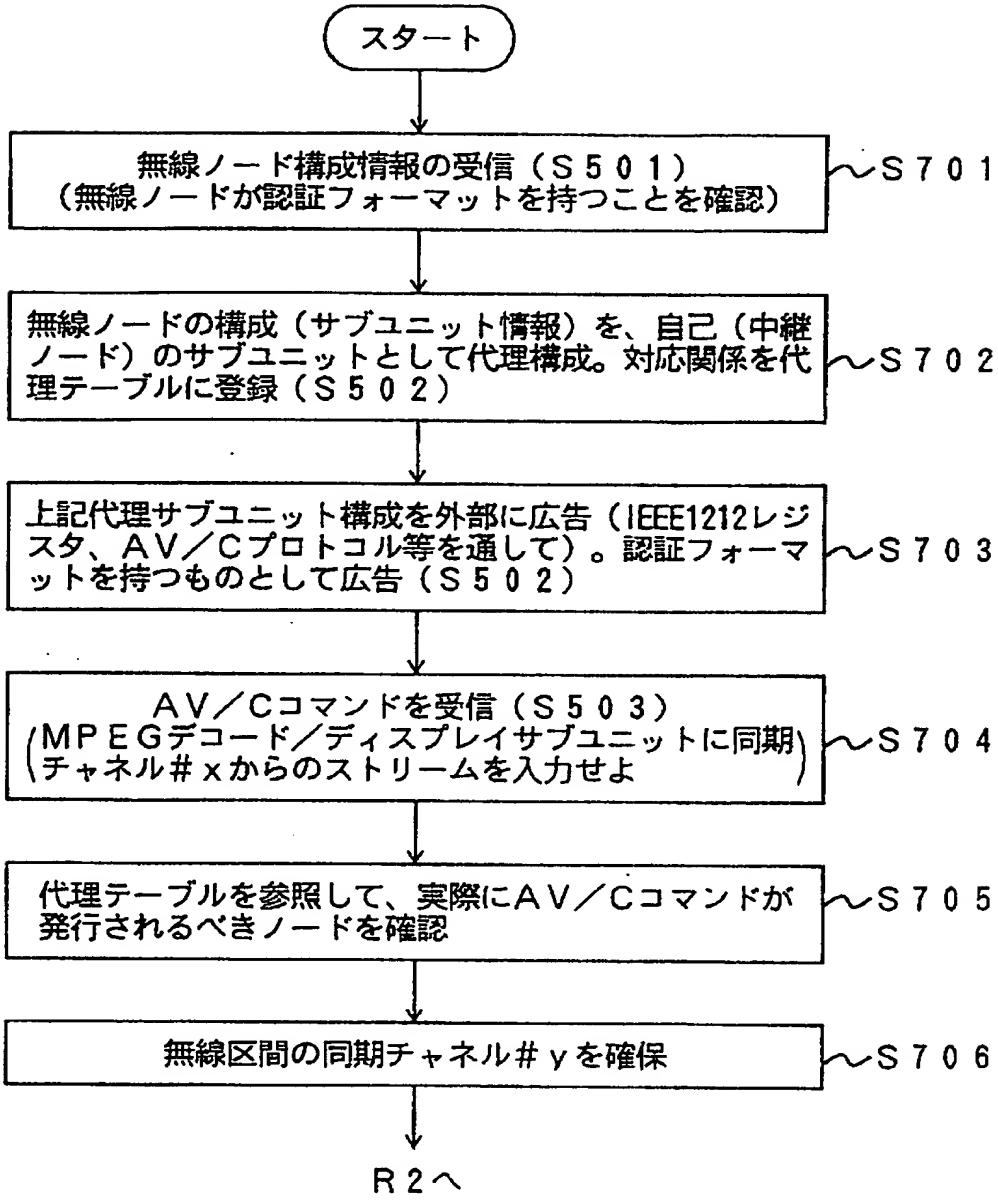
【図７】


スタート
中継ノード102内にMPEGデコード／ディスプレイサブユニットが存在すると認識(S502)
S601
AV/Cプロトコルにて、1394バス上に同期チャネル#xを確立し、これを上記サブユニットに接続して表示せよ、との命令を中継ノード102に送出(S503)
S602
同期チャネル#xを介して、暗号化されたMPEG映像を送出(S506)
S603
認証先問合せ受信。#xの送信先のノード、サブユニット等を記憶し、更に#xにデータを送信しているサブユニットを中継ノードに通知(S523,S524)
S631
認識要求(S509)受信(中継ノードMPEGデコード／ディスプレイサブユニットからの受信と解釈)
S604
Bの認証フォーマットBcertを解き、Bdid等を抽出
S605
中継ノードのMPEGデコード／ディスプレイサブユニットに対して、自らの認証フォーマット(Acert)等をBdidと共に送出(S510)
S606
パケット513を受信(中継ノードのMPEGデコード／ディスプレイサブユニットからの受信と解釈)
S607
タンパの確認、Bcertの確認、認証鍵Kauthの計算
S608
R1へ

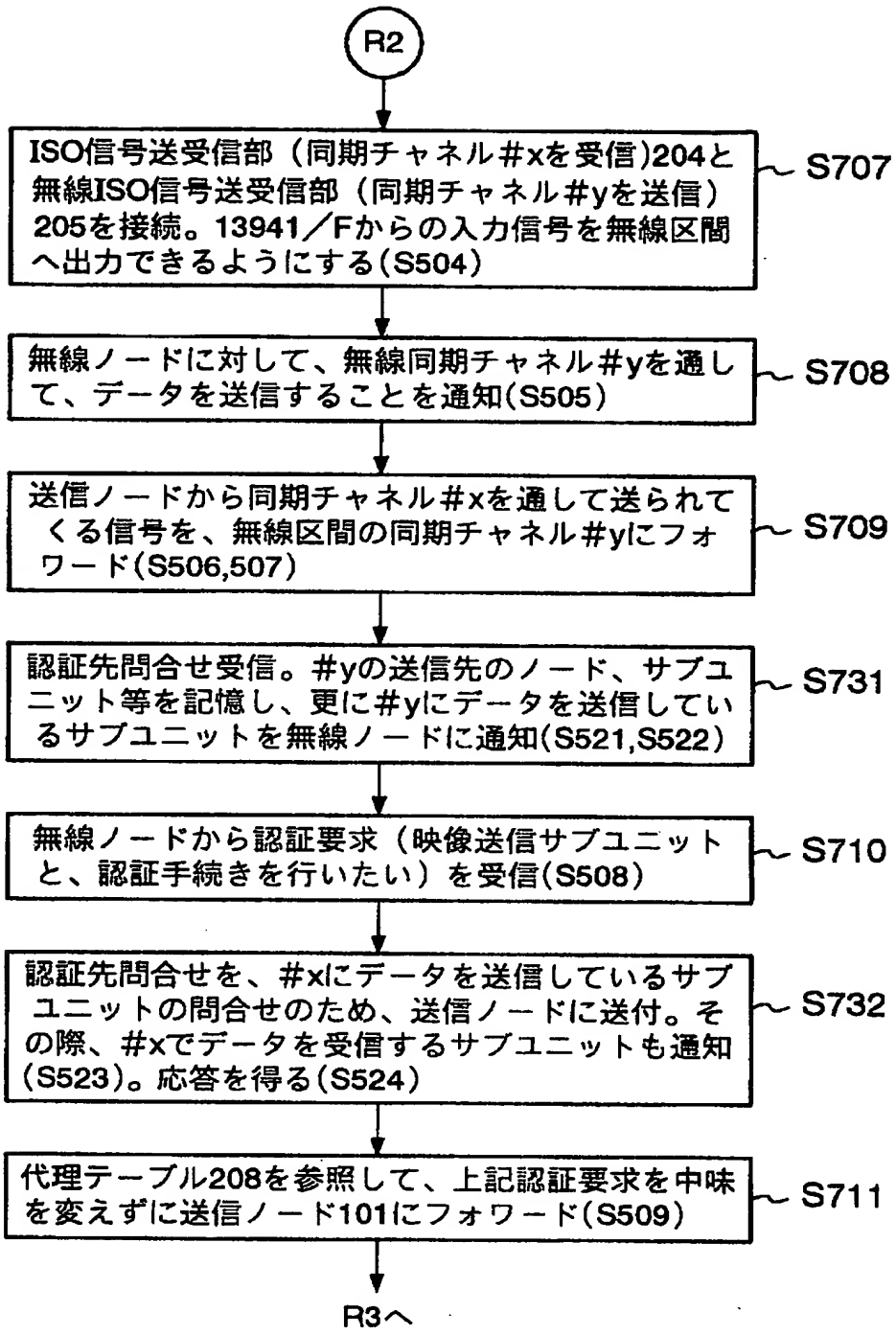
【図８】


R1
中継ノードのMPEGデコード／ディスプレイサブユニットに対して、認証・鍵交換手続き５１４の送信
S609
MPEG映像を鍵Kにて暗号化
S610
暗号化されたMPEG映像［MPEG映像］kを同期チャネル#xを通して送信（S518）
S611

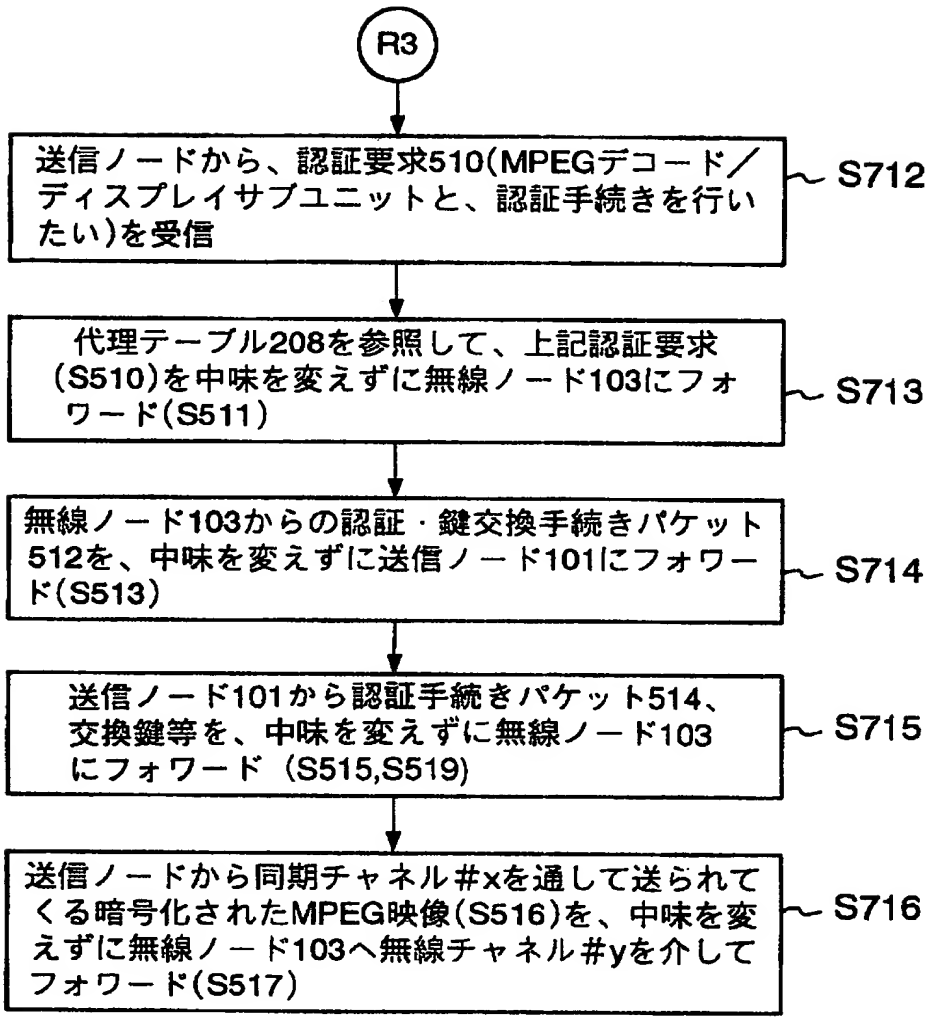
【図９】


スタート
無線ノード構成情報の受信（Ｓ５０１）
（無線ノードが認証フォーマットを持つことを確認）
Ｓ７０１
無線ノードの構成（サブユニット情報）を、自己（中継ノード）のサブユニットとして代理構成。対応関係を代理テーブルに登録（Ｓ５０２）
Ｓ７０２
上記代理サブユニット構成を外部に広告（IEEE1212レジスタ、ＡＶ／Ｃプロトコル等を通して）。認証フォーマットを持つものとして広告（Ｓ５０２）
Ｓ７０３
ＡＶ／Ｃコマンドを受信（Ｓ５０３）
（ＭＰＥＧデコード／ディスプレイサブユニットに同期
チャネル＃ｘからのストリームを入力せよ）
Ｓ７０４
代理テーブルを参照して、実際にＡＶ／Ｃコマンドが発行されるべきノードを確認
Ｓ７０５
無線区間の同期チャネル＃ｙを確保
Ｓ７０６
Ｒ２へ

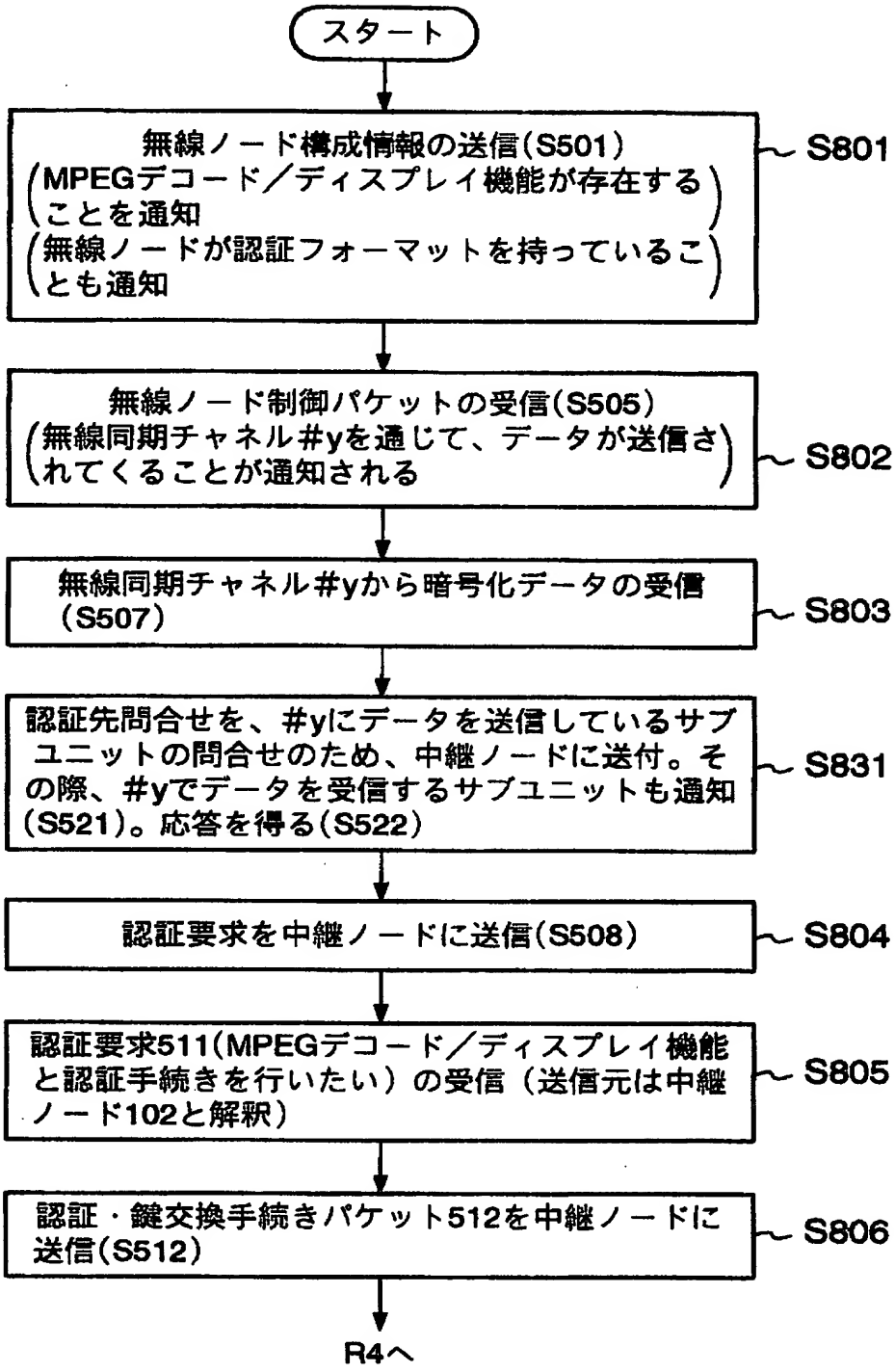
【図１０】


R2
ISO信号送受信部（同期チャネル#xを受信)204と無線ISO信号送受信部（同期チャネル#yを送信）205を接続。13941／Fからの入力信号を無線区間へ出力できるようにする(S504)
S707
無線ノードに対して、無線同期チャネル#yを通して、データを送信することを通知(S505)
S708
送信ノードから同期チャネル#xを通して送られてくる信号を、無線区間の同期チャネル#yにフォワード(S506,507)
S709
認証先問合せ受信。#yの送信先のノード、サブユニット等を記憶し、更に#yにデータを送信しているサブユニットを無線ノードに通知(S521,S522)
S731
無線ノードから認証要求（映像送信サブユニットと、認証手続きを行いたい）を受信(S508)
S710
認証先問合せを、#xにデータを送信しているサブユニットの問合せのため、送信ノードに送付。その際、#xでデータを受信するサブユニットも通知(S523)。応答を得る(S524)
S732
代理テーブル208を参照して、上記認証要求を中味を変えずに送信ノード101にフォワード(S509)
S711
R3へ

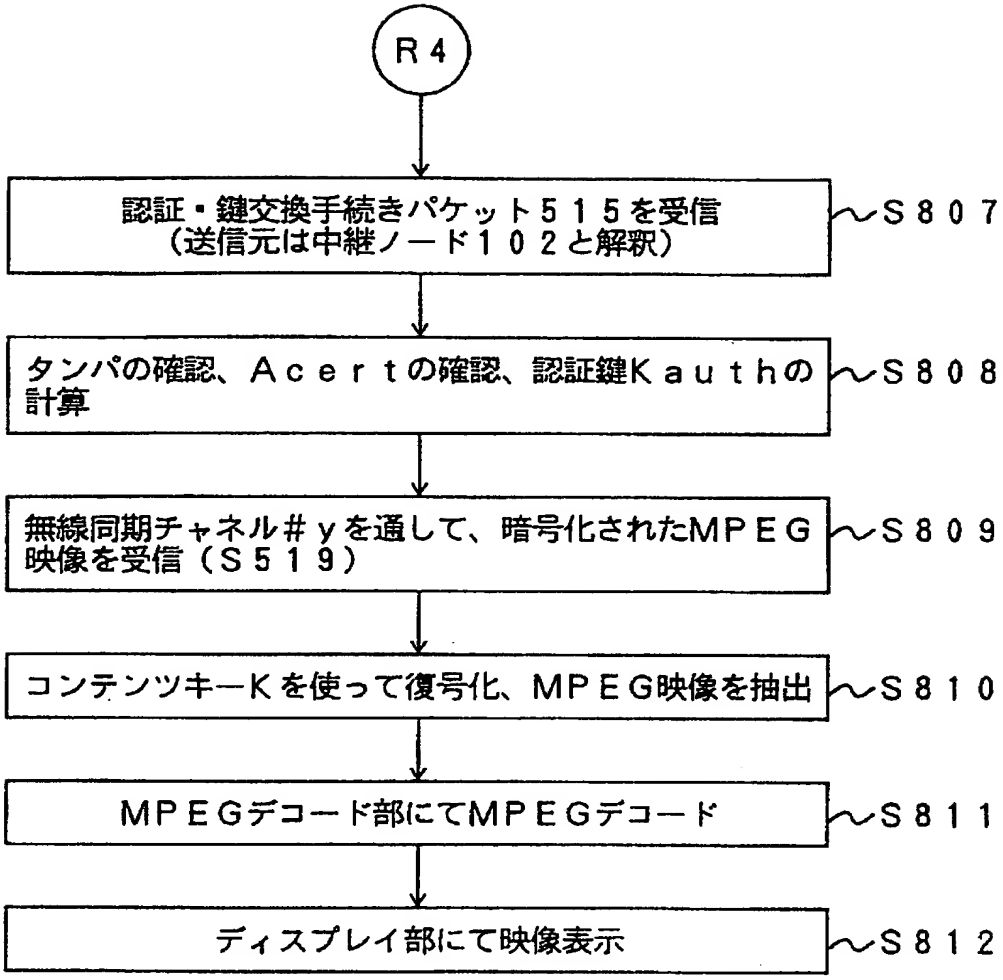
【図１１】


R3
送信ノードから、認証要求510(MPEGデコード／ディスプレイサブユニットと、認証手続きを行いたい)を受信
S712
代理テーブル208を参照して、上記認証要求(S510)を中味を変えずに無線ノード103にフォワード(S511)
S713
無線ノード103からの認証・鍵交換手続きパケット512を、中味を変えずに送信ノード101にフォワード(S513)
S714
送信ノード101から認証手続きパケット514、交換鍵等を、中味を変えずに無線ノード103にフォワード (S515,S519)
S715
送信ノードから同期チャネル#xを通して送られてくる暗号化されたMPEG映像(S516)を、中味を変えずに無線ノード103へ無線チャネル#yを介してフォワード(S517)
S716

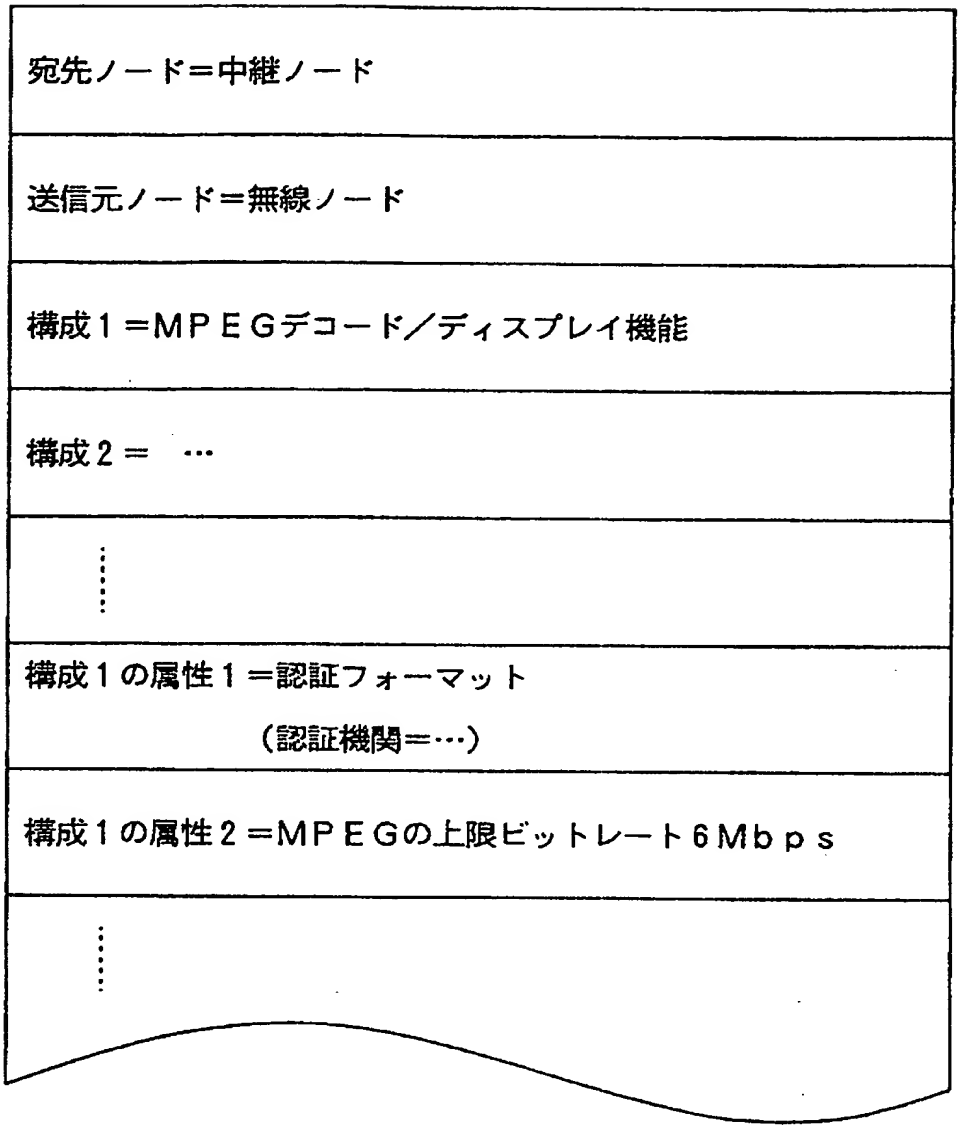
【図１２】


スタート
無線ノード構成情報の送信(S501)
(MPEGデコード／ディスプレイ機能が存在することを通知
(無線ノードが認証フォーマットを持っていることも通知
S801
無線ノード制御パケットの受信(S505)
(無線同期チャネル#yを通じて、データが送信されてくることが通知される
S802
無線同期チャネル#yから暗号化データの受信(S507)
S803
認証先問合せを、#yにデータを送信しているサブユニットの問合せのため、中継ノードに送付。その際、#yでデータを受信するサブユニットも通知(S521)。応答を得る(S522)
S831
認証要求を中継ノードに送信(S508)
S804
認証要求511(MPEGデコード／ディスプレイ機能と認証手続きを行いたい）の受信（送信元は中継ノード102と解釈)
S805
認証・鍵交換手続きパケット512を中継ノードに送信(S512)
S806
R4へ

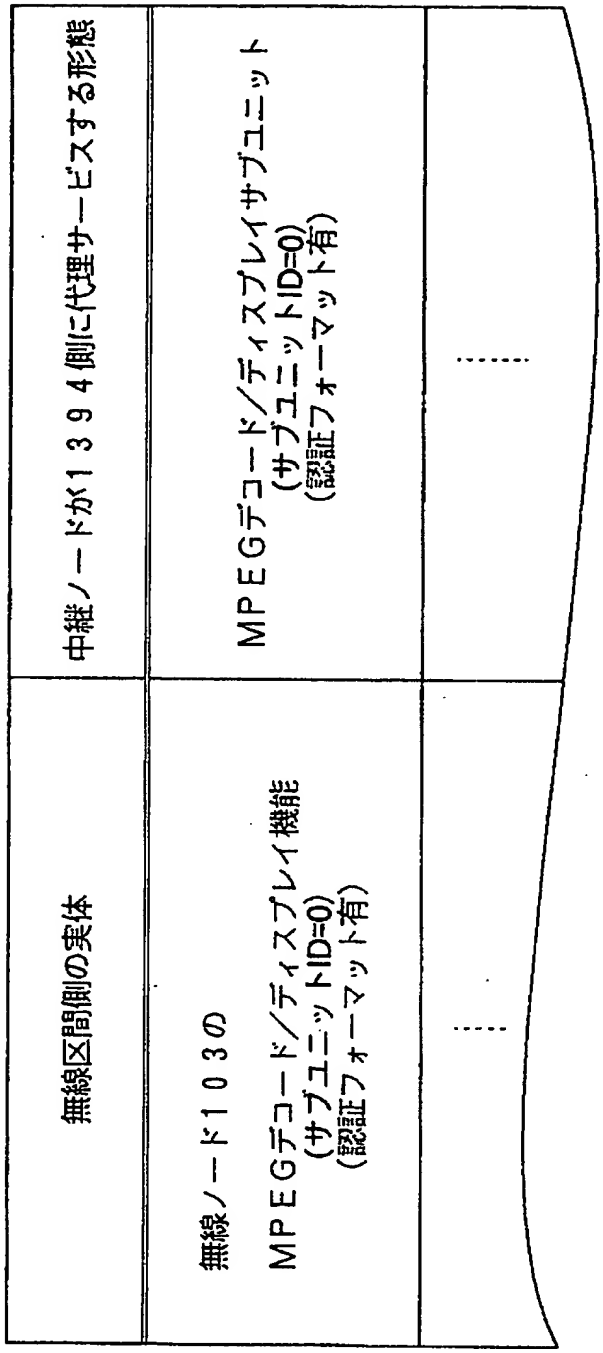
【図１３】


R4
認証・鍵交換手続きパケット５１５を受信
（送信元は中継ノード１０２と解釈）
～Ｓ８０７
タンパの確認、Ａｃｅｒｔの確認、認証鍵Ｋａｕｔｈの計算
～Ｓ８０８
無線同期チャネル＃ｙを通して、暗号化されたＭＰＥＧ映像を受信（Ｓ５１９）
～Ｓ８０９
コンテンツキーＫを使って復号化、ＭＰＥＧ映像を抽出
～Ｓ８１０
ＭＰＥＧデコード部にてＭＰＥＧデコード
～Ｓ８１１
ディスプレイ部にて映像表示
～Ｓ８１２

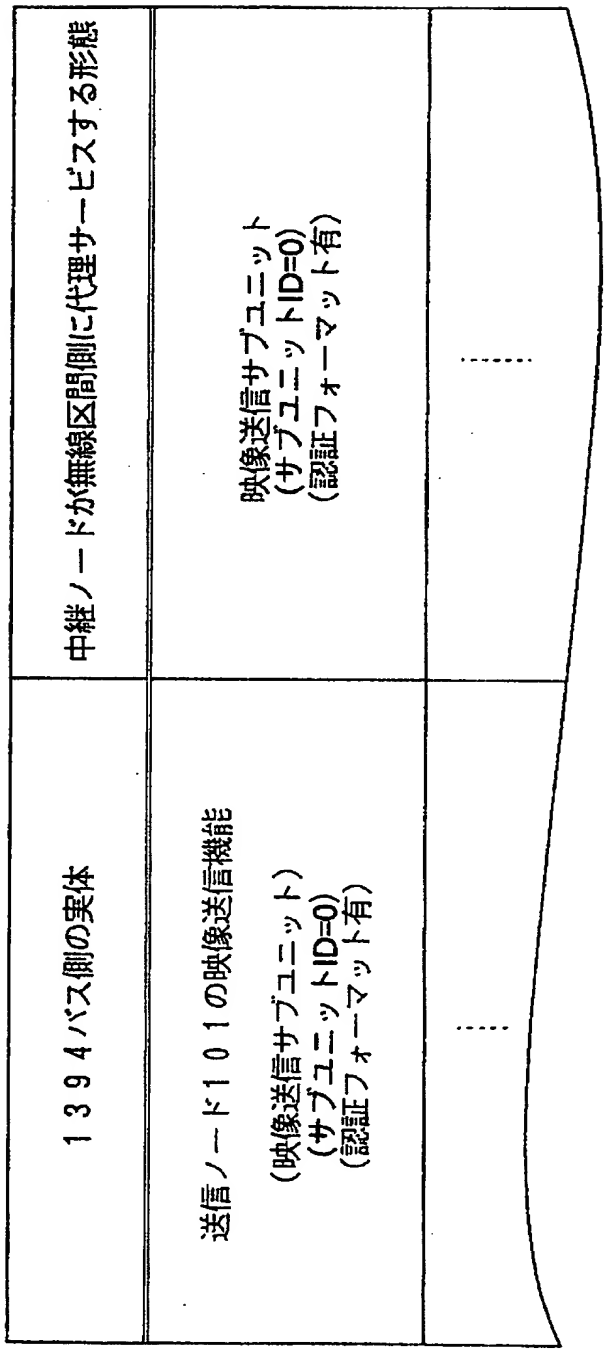
【図１４】


宛先ノード＝中継ノード
送信元ノード＝無線ノード
構成１＝ＭＰＥＧデコード／ディスプレイ機能
構成２＝　…
構成１の属性１＝認証フォーマット
（認証機関＝…）
構成１の属性２＝ＭＰＥＧの上限ビットレート６Ｍｂｐｓ

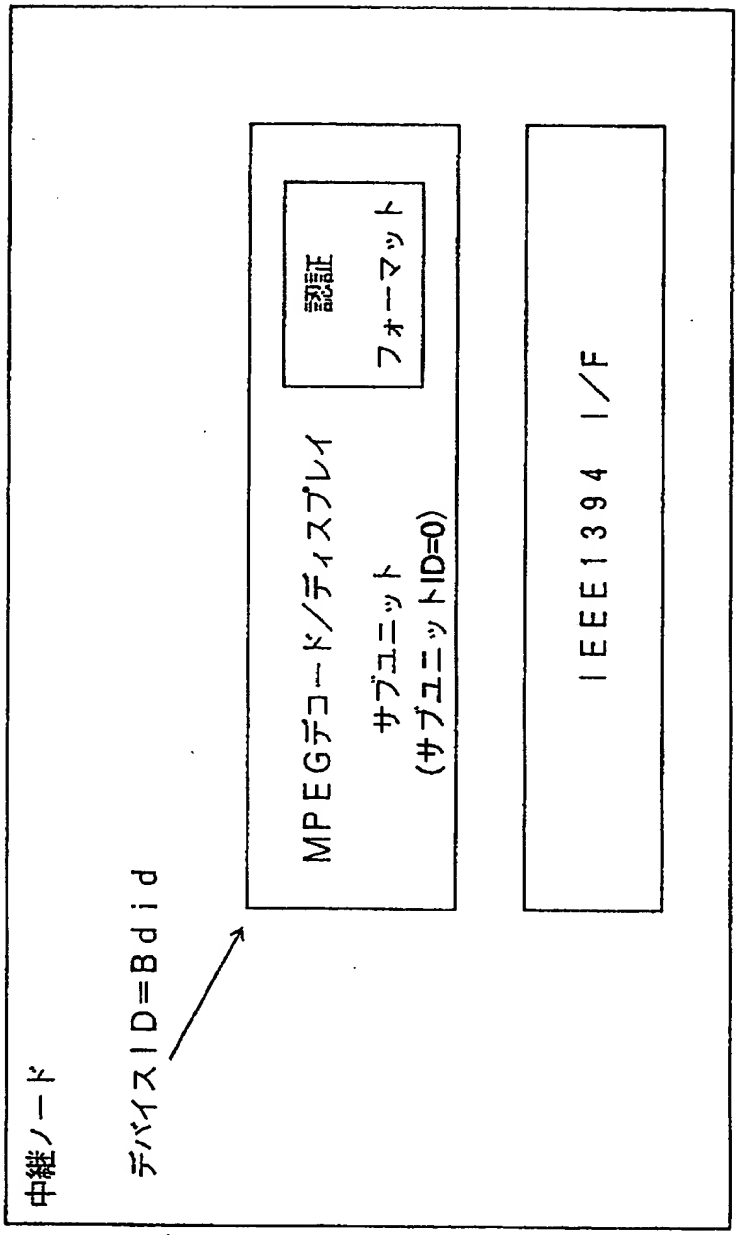
【図１５】


無線区間側の実体
中継ノードが１３９４側に代理サービスする形態
無線ノード１０３の
MPEGデコード／ディスプレイ機能
(サブユニットID=0)
(認証フォーマット有)
MPEGデコード／ディスプレイサブユニット
(サブユニットID=0)
(認証フォーマット有)

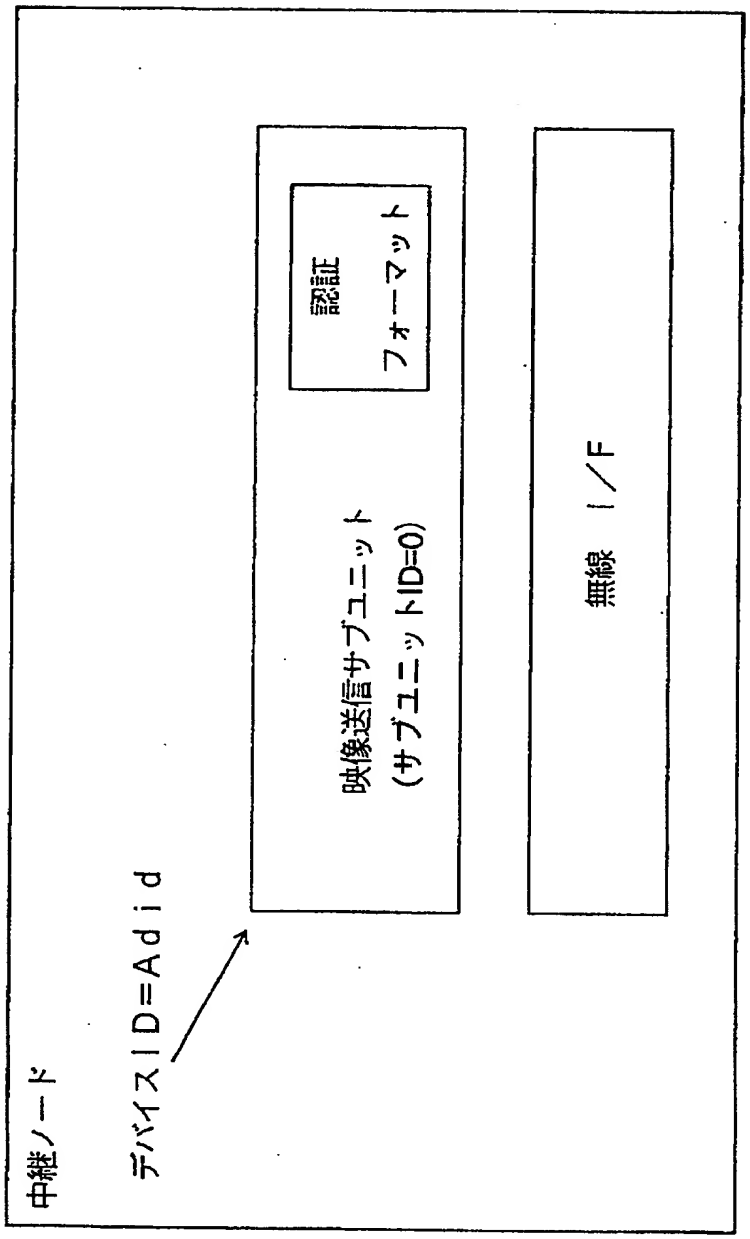
【図１６】


１３９４バス側の実体
中継ノードが無線区間側に代理サービスする形態
送信ノード１０１の映像送信機能
(映像送信サブユニット)
(サブユニットID=0)
(認証フォーマット有)
映像送信サブユニット
(サブユニットID=0)
(認証フォーマット有)

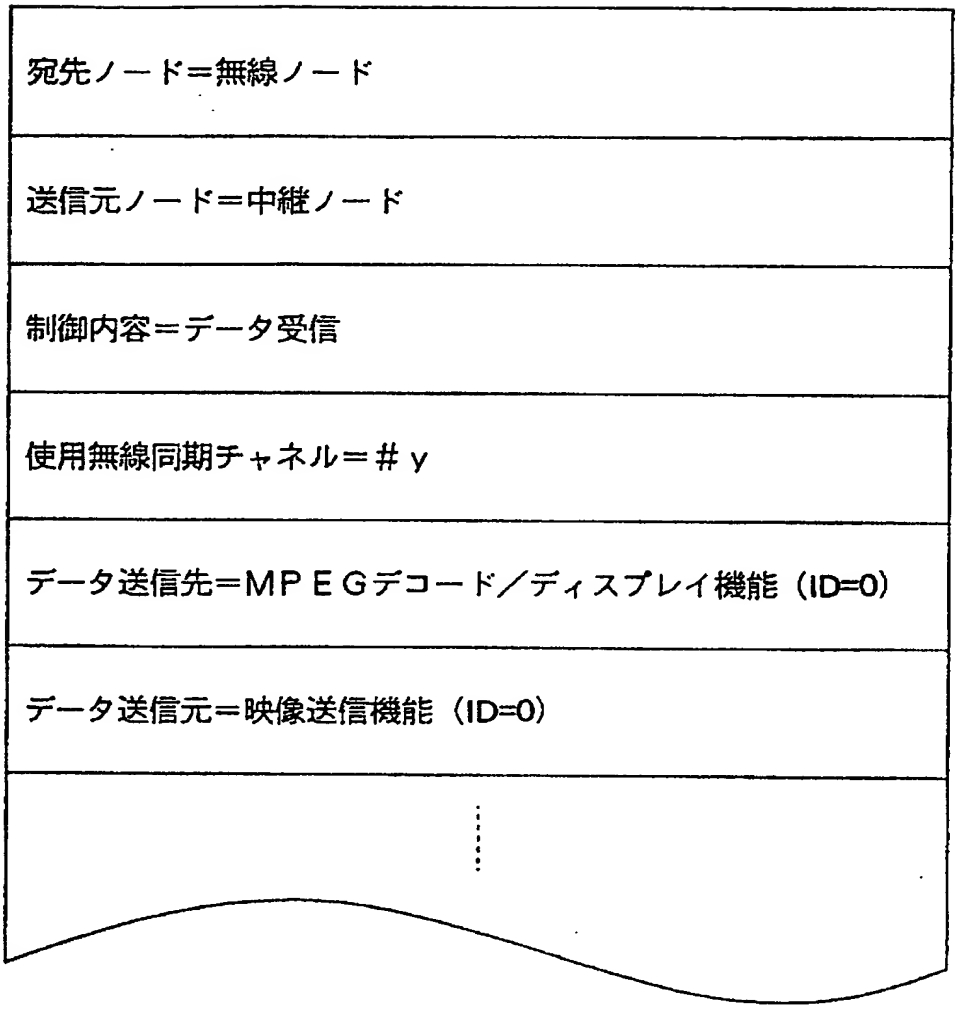
【図１７】


中継ノード
デバイスID=Bdid
MPEGデコード／ディスプレイ
サブユニット
(サブユニットID=0)
認証
フォーマット
IEEE1394 I／F

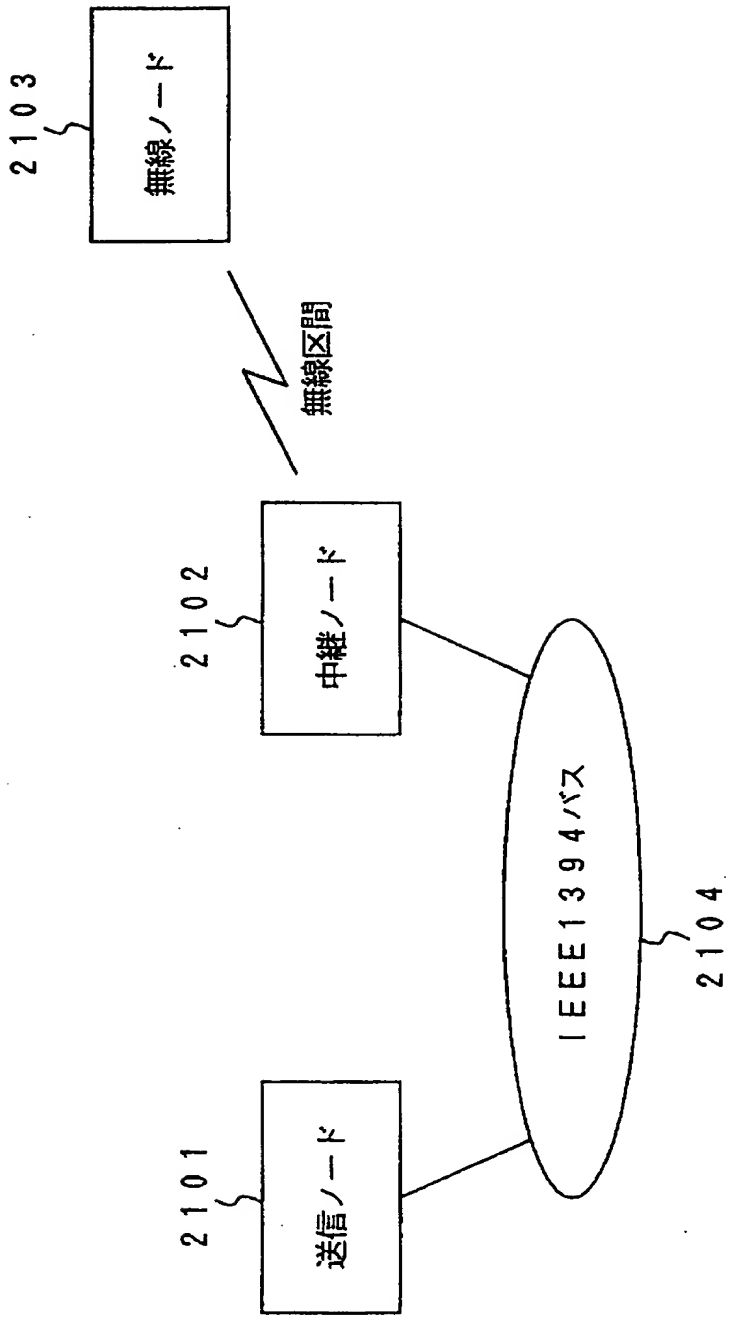
【図１８】



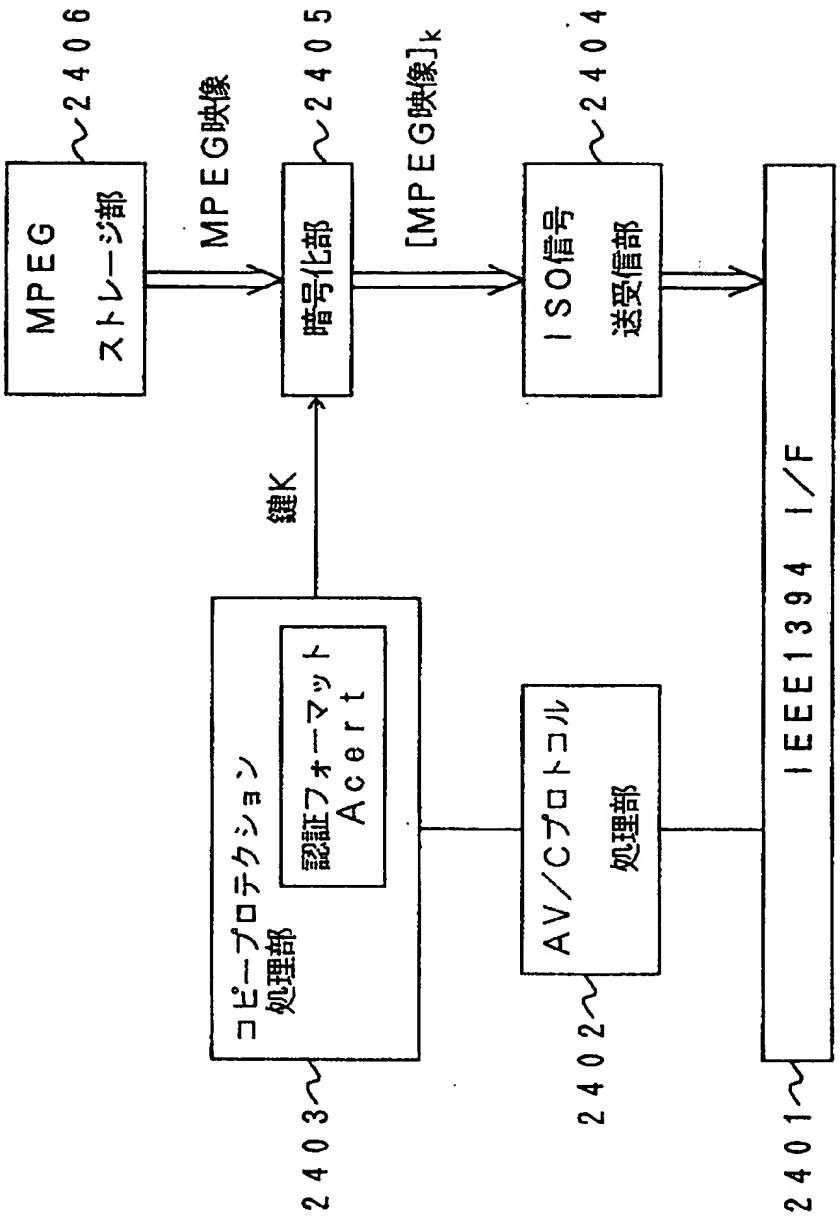
【図１９】


宛先ノード＝無線ノード
送信元ノード＝中継ノード
制御内容＝データ受信
使用無線同期チャネル＝＃ｙ
データ送信先＝ＭＰＥＧデコード／ディスプレイ機能（ID=0）
データ送信元＝映像送信機能（ID=0）

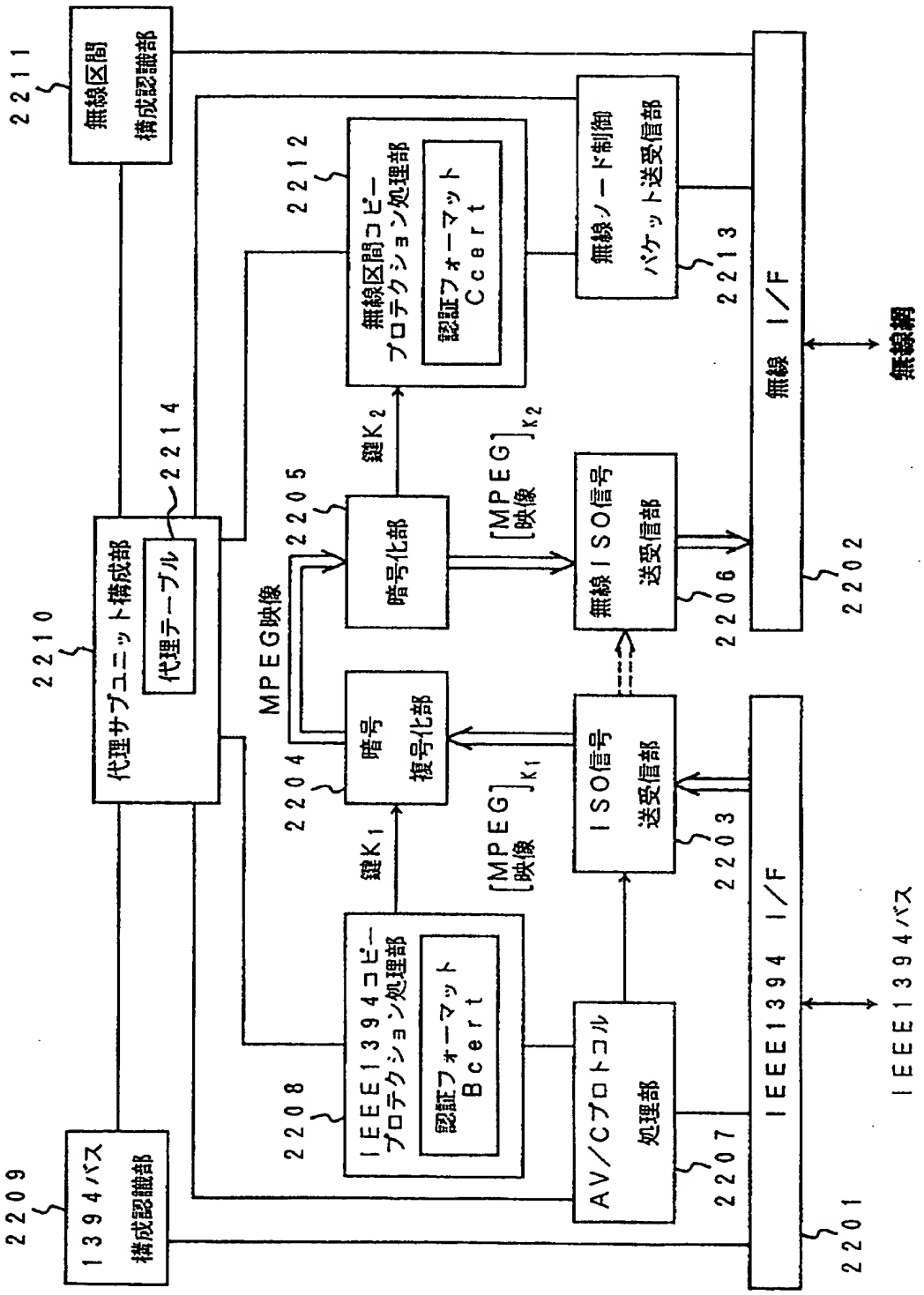
【図２０】



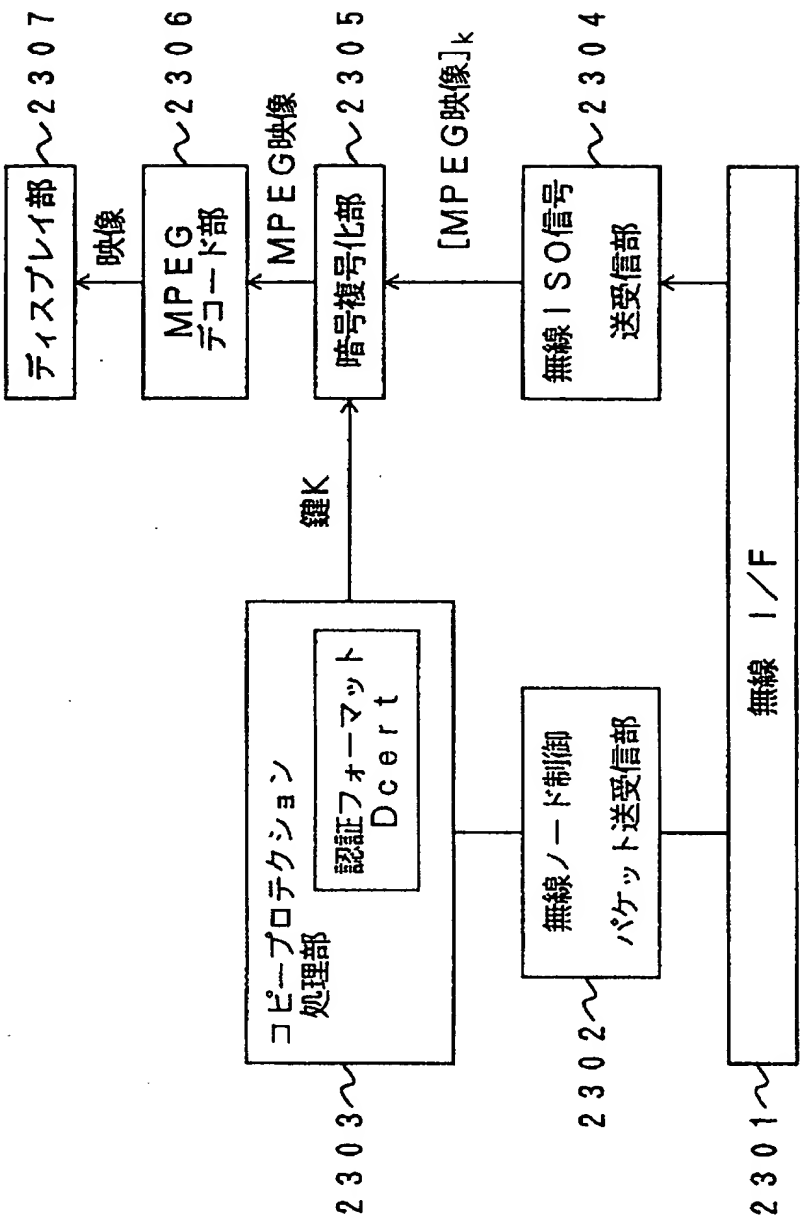
【図２１】


MPEG
ストレージ部
2406
MPEG映像
暗号化部
2405
[MPEG映像]k
ISO信号
送受信部
2404
鍵K
コピープロテクション
処理部
認証フォーマット
Acert
2403
AV／Cプロトコル
処理部
2402
IEEE1394 I／F
2401

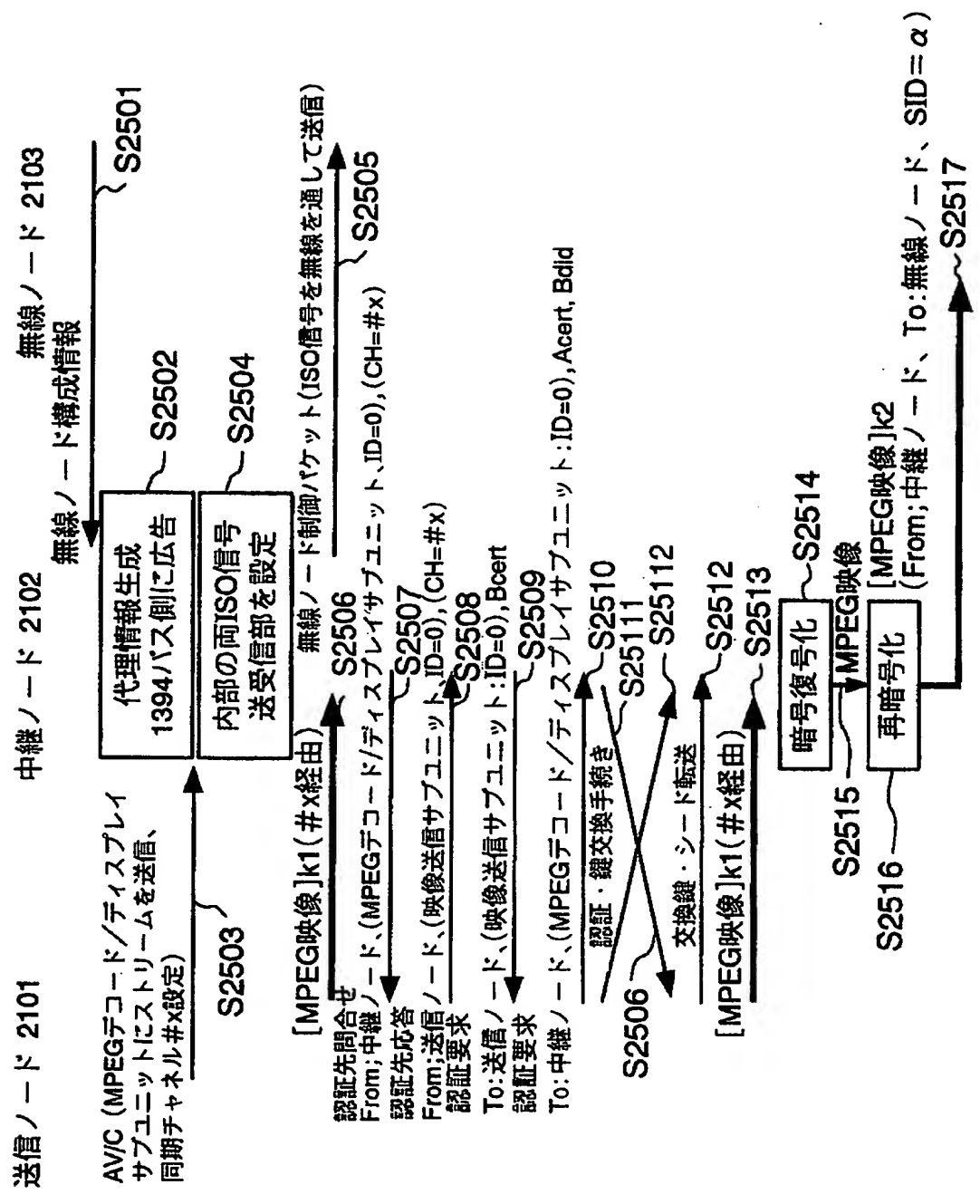
【図２２】


無線区間構成認識部
2211
無線区間コピープロテクション処理部
2212
認証フォーマット Ccert
無線ノード制御パケット送受信部
2213
無線 I／F
2202
無線網
代理サブユニット構成部
2210
代理テーブル
2214
MPEG映像
2205
暗号化部
鍵K2
[MPEG映像]K2
無線ISO信号送受信部
2206
暗号複号化部
2204
鍵K1
[MPEG映像]K1
ISO信号送受信部
2203
IEEE1394コピープロテクション処理部
2208
認証フォーマット Bcert
AV／Cプロトコル処理部
2207
IEEE1394 I／F
2201
IEEE1394バス
1394バス構成認識部
2209

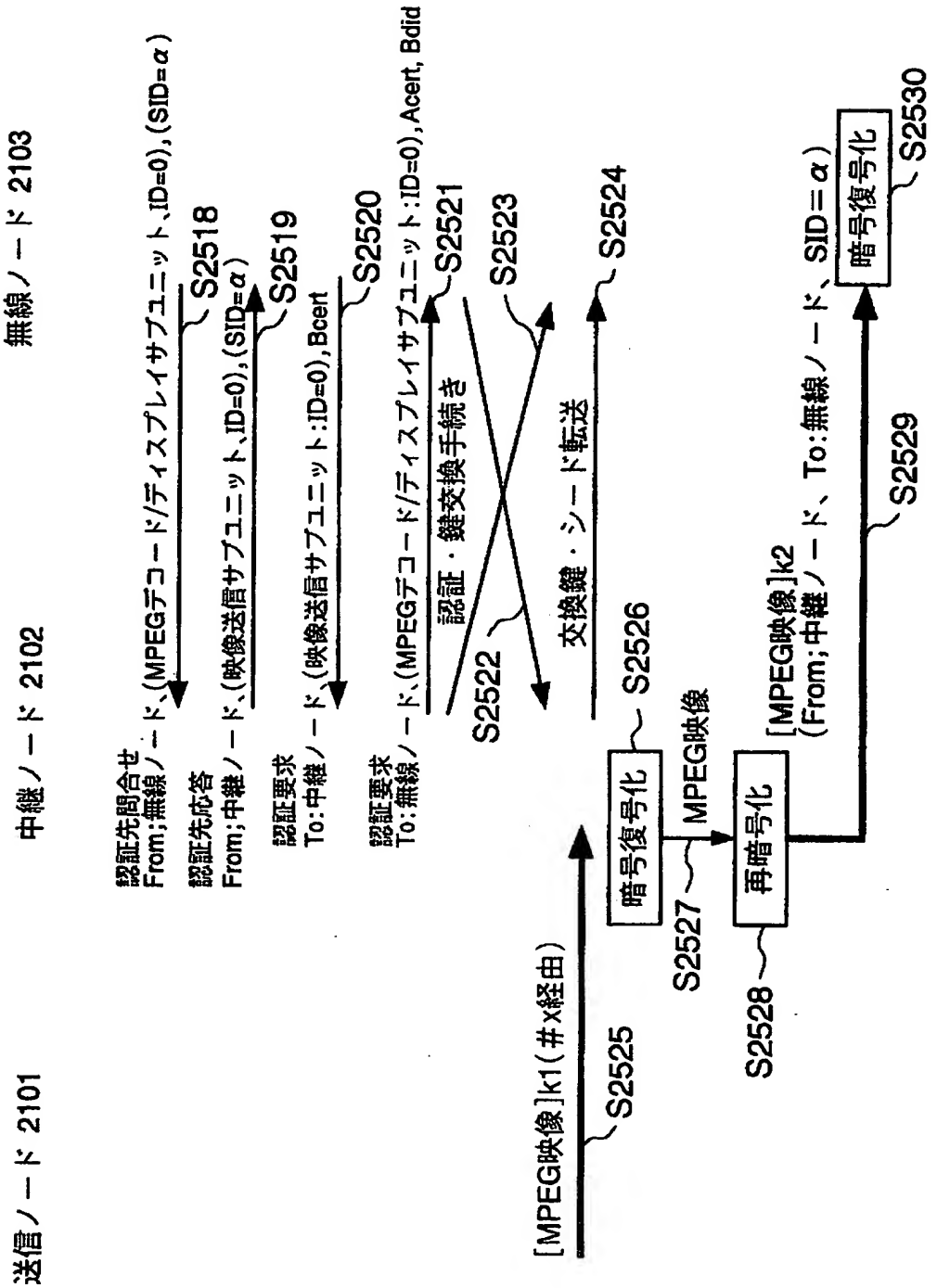
【図２３】


ディスプレイ部
2307
映像
MPEG
デコード部
2306
MPEG映像
暗号複号化部
2305
[MPEG映像]k
無線ISO信号
送受信部
2304
鍵K
コピープロテクション
処理部
認証フォーマット
Dcert
2303
無線ノード制御
パケット送受信部
2302
無線 I/F
2301

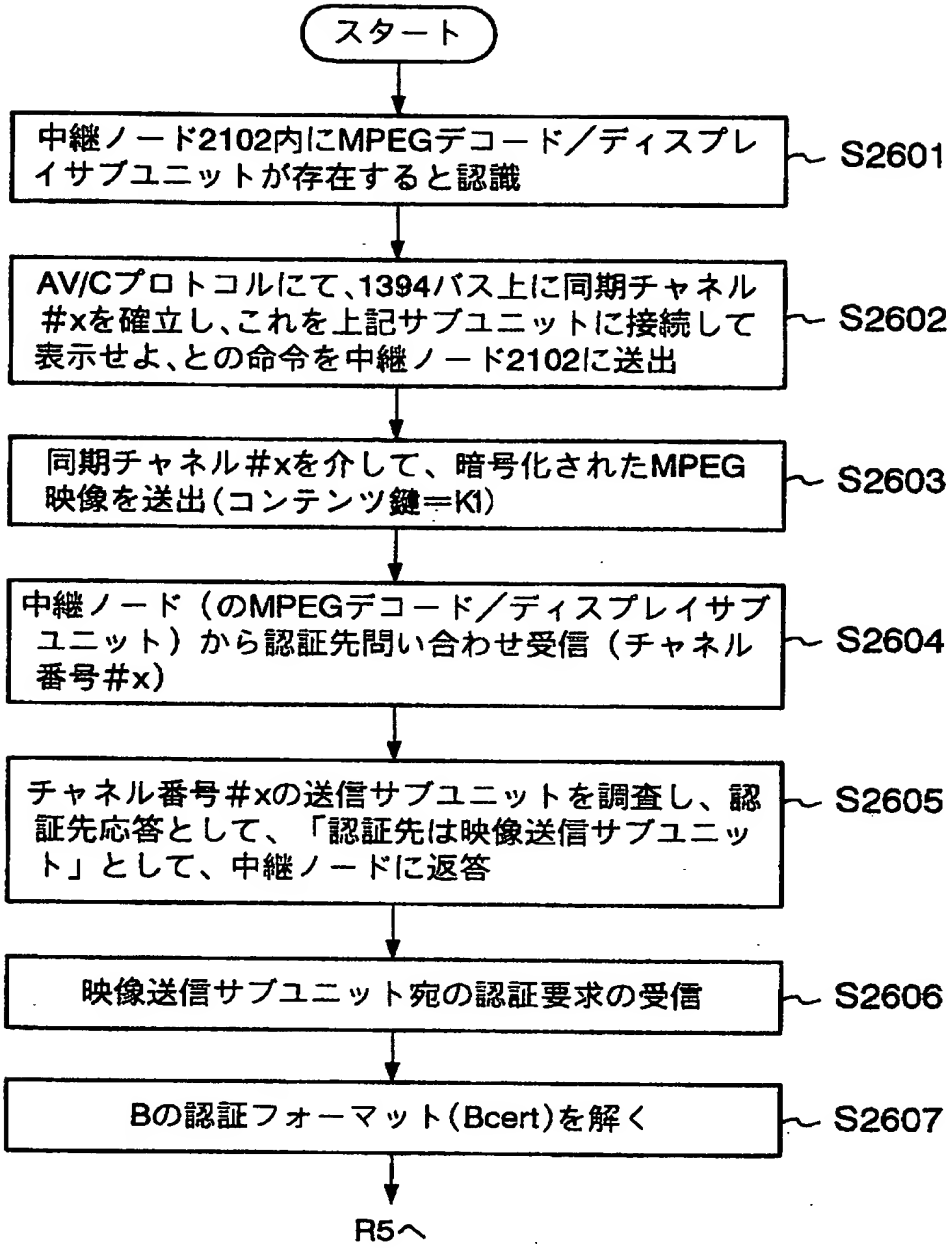
【図２４】


送信ノード 2101
中継ノード 2102
無線ノード 2103
無線ノード構成情報
S2501
代理情報生成
1394バス側に広告
S2502
内部のISO信号
送受信部を設定
S2504
AV/C (MPEGデコード/ディスプレイ
サブユニットにストリームを送信、
同期チャネル#x設定)
S2503
[MPEG映像]k1(#x経由)
無線ノード制御パケット(ISO信号を無線を通して送信)
S2505
認証先問合せ
From;中継ノード、(MPEGデコード/ディスプレイサブユニット、ID=0),(CH=#x)
S2506
認証先応答
From;送信ノード、(映像送信サブユニット、ID=0),(CH=#x)
S2507
認証要求
To:送信ノード、(映像送信サブユニット:ID=0),Bcert
S2508
認証要求
To:中継ノード、(MPEGデコード/ディスプレイサブユニット:ID=0),Acert, Bdid
S2509
認証・鍵交換手続き
S2506
S2510
S25111
交換鍵・シード転送
S25112
[MPEG映像]k1(#x経由)
S2512
S2513
暗号復号化
S2514
MPEG映像
S2515
再暗号化
[MPEG映像]k2
(From;中継ノード、To:無線ノード、SID=α)
S2516
S2517

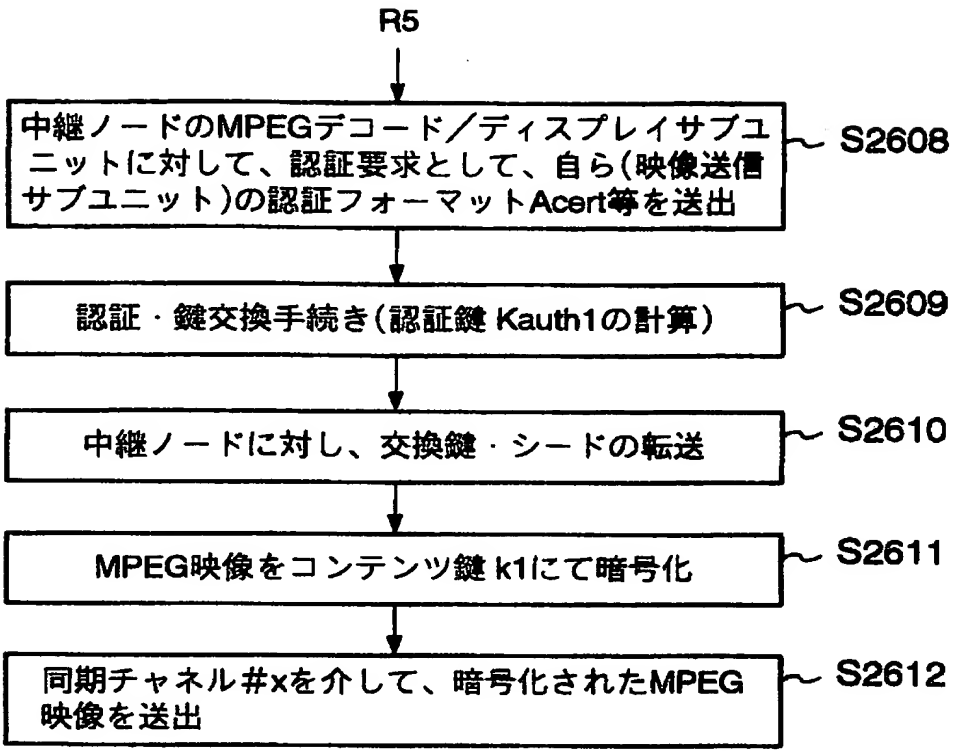
【図２５】


送信ノード 2101
中継ノード 2102
無線ノード 2103
認証先問合せ
From;無線ノード、(MPEGデコード/ディスプレイサブユニット、ID=0),(SID=α)
S2518
認証先応答
From;中継ノード、(映像送信サブユニット、ID=0),(SID=α)
S2519
認証要求
To:中継ノード、(映像送信サブユニット:ID=0),Bcert
S2520
認証要求
To:無線ノード、(MPEGデコード/ディスプレイサブユニット:ID=0),Acert, Bdid
S2521
認証・鍵交換手続き
S2522
S2523
交換鍵・シード転送
S2524
[MPEG映像]k1(#x経由)
S2525
暗号復号化
S2526
MPEG映像
S2527
再暗号化
S2528
[MPEG映像]k2
(From;中継ノード、To:無線ノード、SID=α)
S2529
暗号復号化
S2530

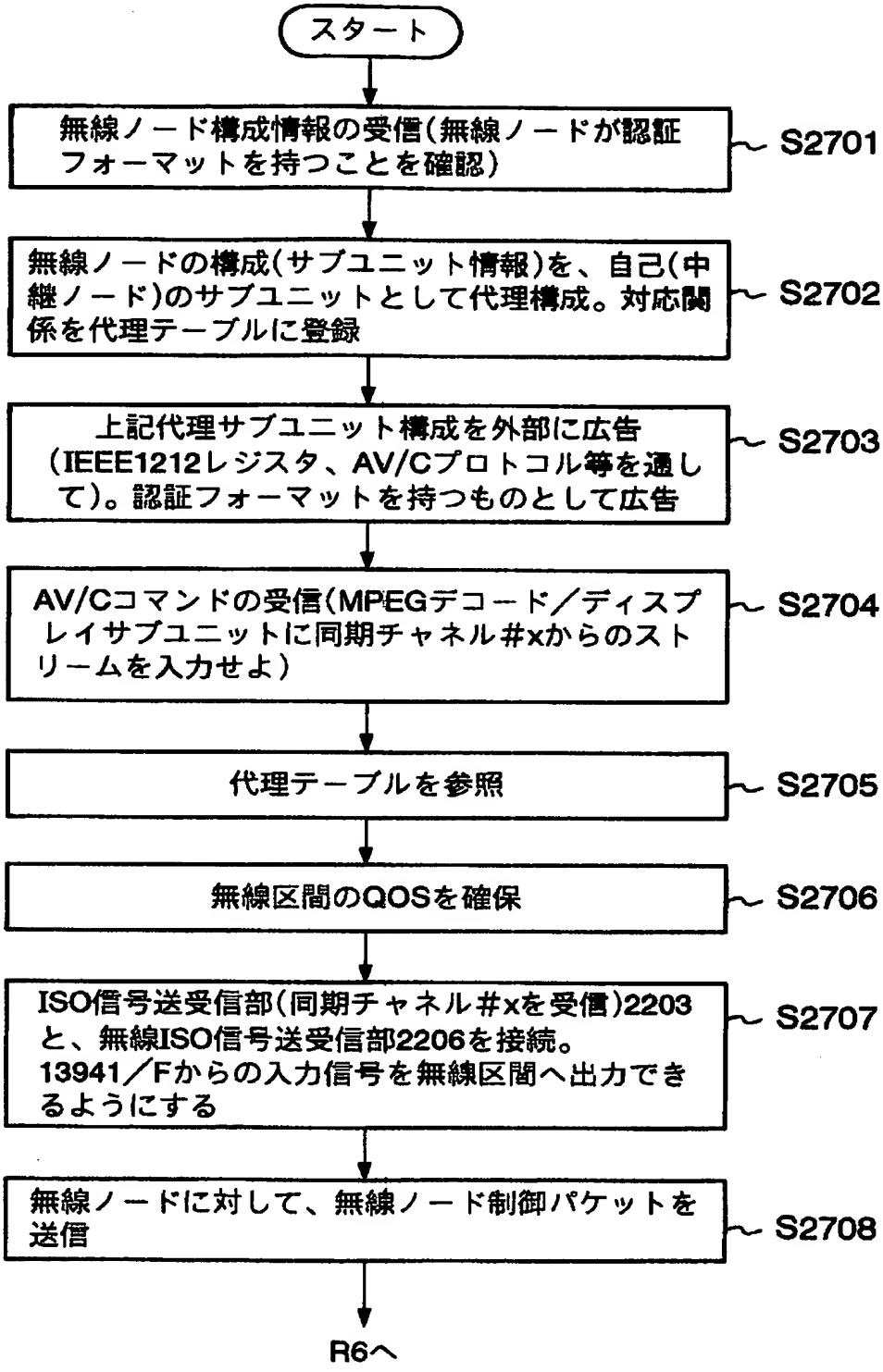
【図２６】


スタート
中継ノード2102内にMPEGデコード／ディスプレイサブユニットが存在すると認識
S2601
AV/Cプロトコルにて、1394バス上に同期チャネル#xを確立し、これを上記サブユニットに接続して表示せよ、との命令を中継ノード2102に送出
S2602
同期チャネル#xを介して、暗号化されたMPEG映像を送出(コンテンツ鍵＝Ki)
S2603
中継ノード（のMPEGデコード／ディスプレイサブユニット）から認証先問い合わせ受信（チャネル番号#x）
S2604
チャネル番号#xの送信サブユニットを調査し、認証先応答として、「認証先は映像送信サブユニット」として、中継ノードに返答
S2605
映像送信サブユニット宛の認証要求の受信
S2606
Bの認証フォーマット(Bcert)を解く
S2607
R5へ

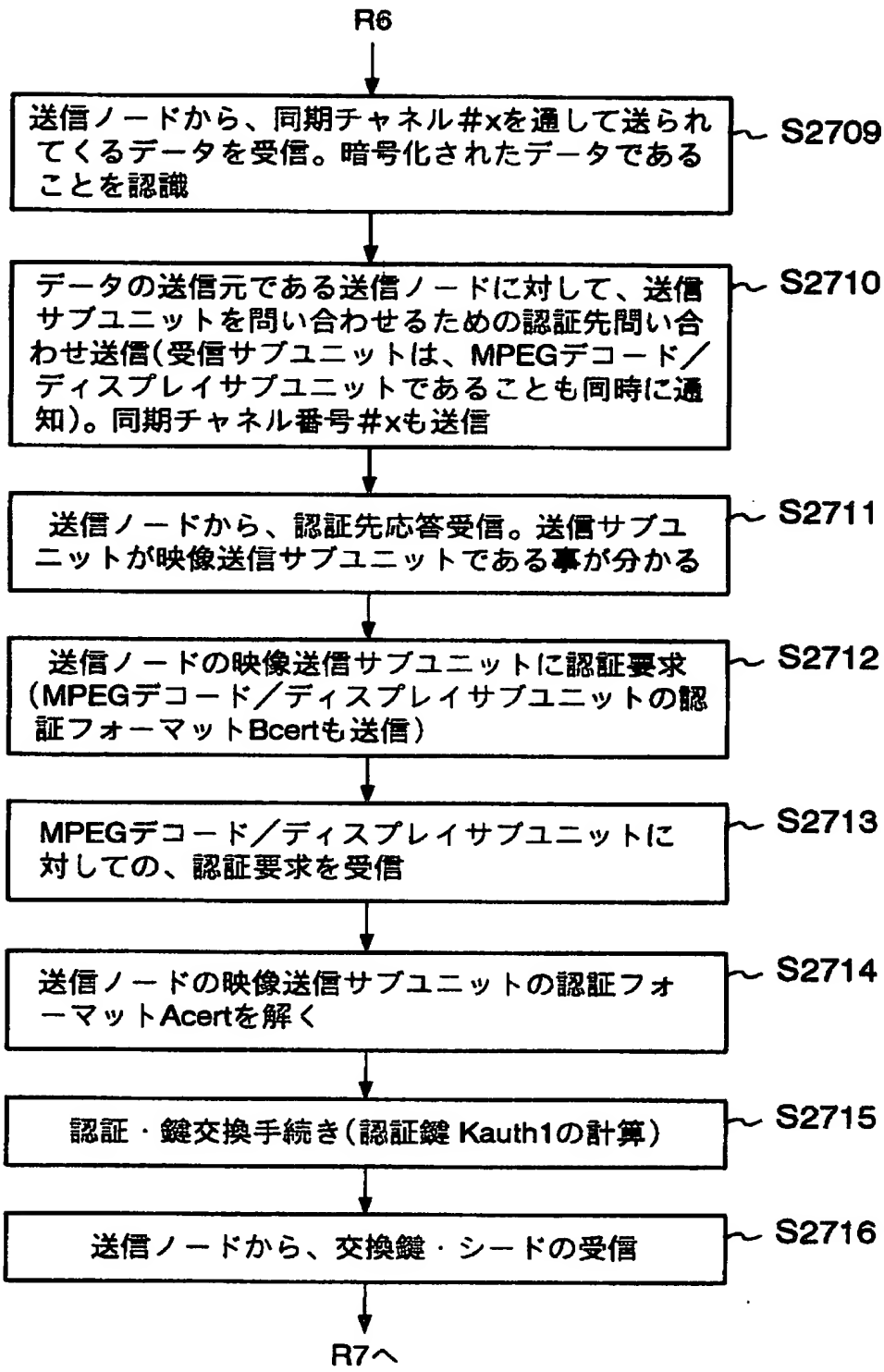
【図２７】


R5
中継ノードのMPEGデコード／ディスプレイサブユニットに対して、認証要求として、自ら(映像送信サブユニット)の認証フォーマットAcert等を送出
S2608
認証・鍵交換手続き(認証鍵 Kauth1の計算)
S2609
中継ノードに対し、交換鍵・シードの転送
S2610
MPEG映像をコンテンツ鍵 k1にて暗号化
S2611
同期チャネル#xを介して、暗号化されたMPEG映像を送出
S2612

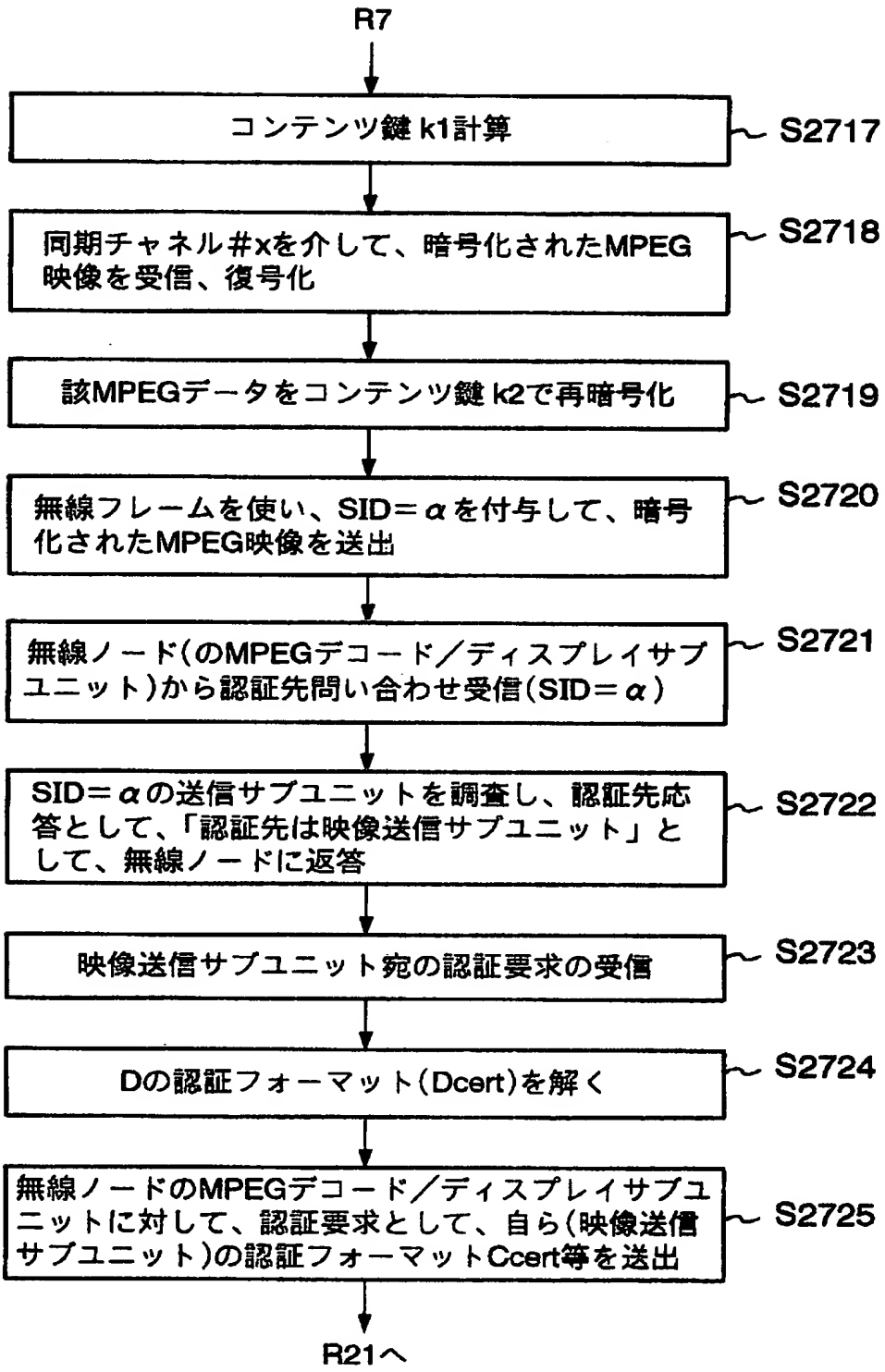
【図２８】


スタート
無線ノード構成情報の受信(無線ノードが認証フォーマットを持つことを確認)
S2701
無線ノードの構成(サブユニット情報)を、自己(中継ノード)のサブユニットとして代理構成。対応関係を代理テーブルに登録
S2702
上記代理サブユニット構成を外部に広告(IEEE1212レジスタ、AV/Cプロトコル等を通して)。認証フォーマットを持つものとして広告
S2703
AV/Cコマンドの受信(MPEGデコード／ディスプレイサブユニットに同期チャネル#xからのストリームを入力せよ)
S2704
代理テーブルを参照
S2705
無線区間のQOSを確保
S2706
ISO信号送受信部(同期チャネル#xを受信)2203と、無線ISO信号送受信部2206を接続。13941／Fからの入力信号を無線区間へ出力できるようにする
S2707
無線ノードに対して、無線ノード制御パケットを送信
S2708
R6へ

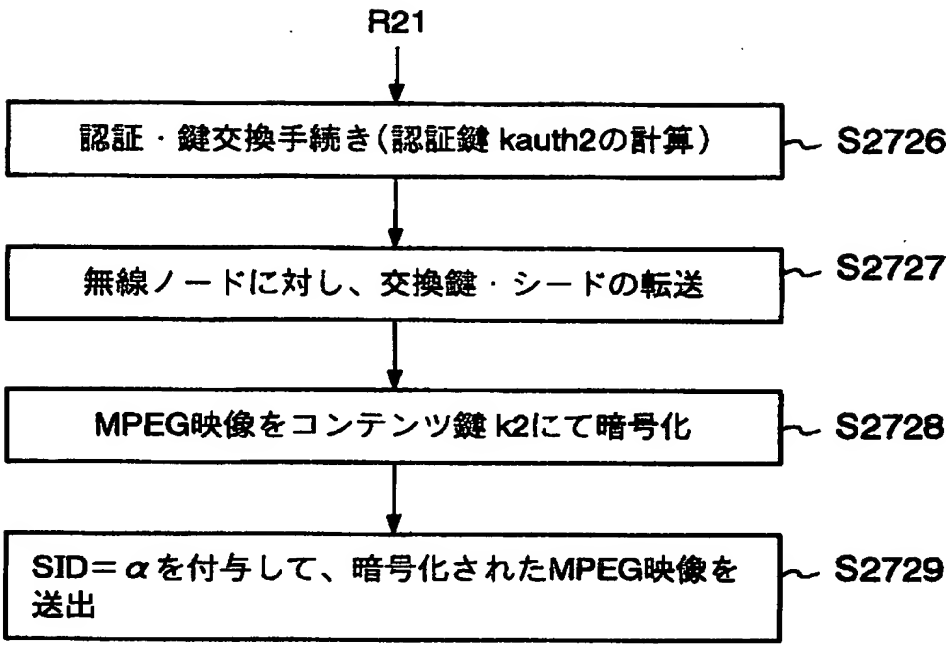
【図２９】


R6
送信ノードから、同期チャネル#xを通して送られてくるデータを受信。暗号化されたデータであることを認識
S2709
データの送信元である送信ノードに対して、送信サブユニットを問い合わせるための認証先問い合わせ送信(受信サブユニットは、MPEGデコード／ディスプレイサブユニットであることも同時に通知)。同期チャネル番号#xも送信
S2710
送信ノードから、認証先応答受信。送信サブユニットが映像送信サブユニットである事が分かる
S2711
送信ノードの映像送信サブユニットに認証要求(MPEGデコード／ディスプレイサブユニットの認証フォーマットBcertも送信)
S2712
MPEGデコード／ディスプレイサブユニットに対しての、認証要求を受信
S2713
送信ノードの映像送信サブユニットの認証フォーマットAcertを解く
S2714
認証・鍵交換手続き(認証鍵 Kauth1の計算)
S2715
送信ノードから、交換鍵・シードの受信
S2716
R7へ

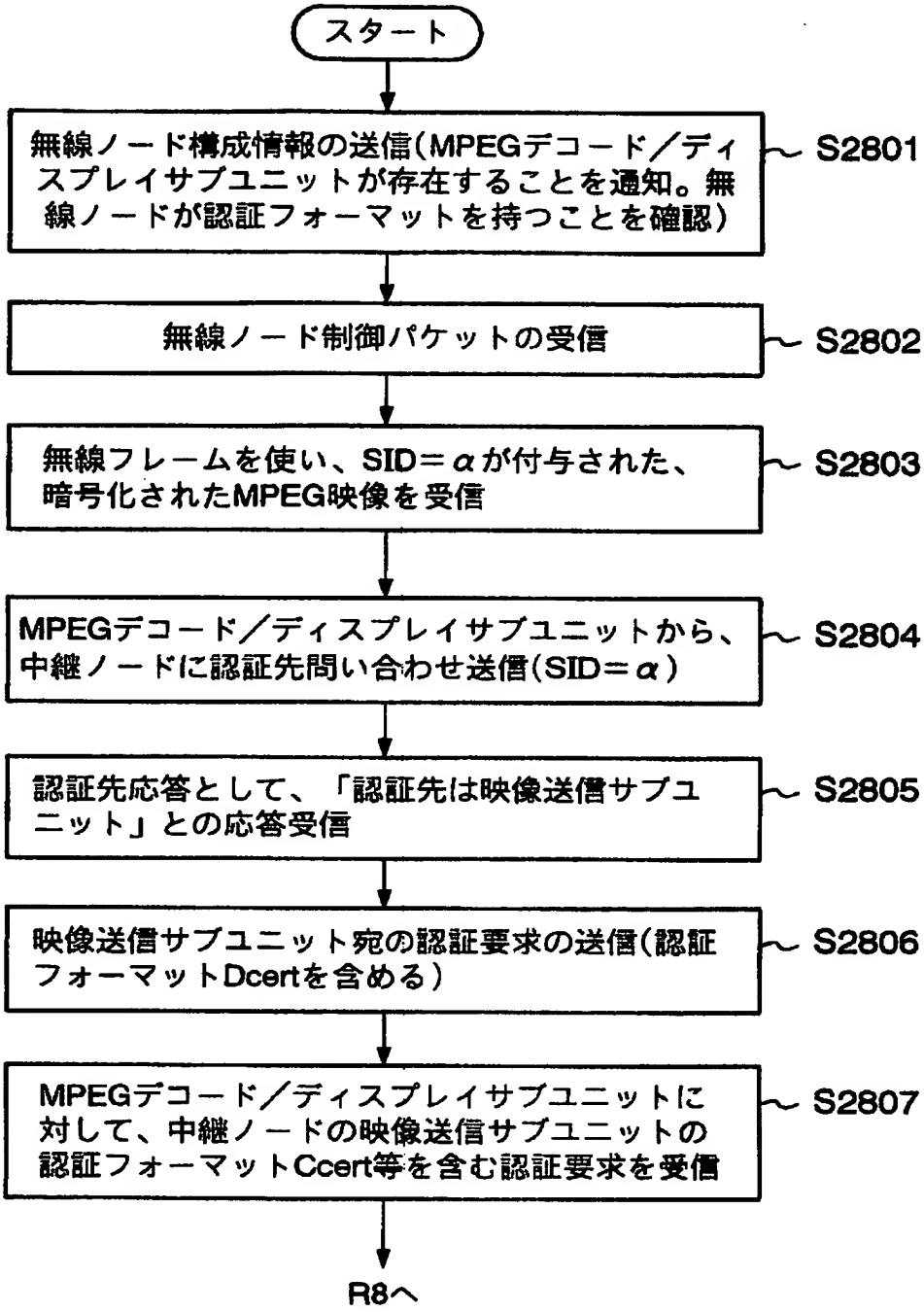
【図３０】


R7
コンテンツ鍵k1計算
S2717
同期チャネル#xを介して、暗号化されたMPEG映像を受信、復号化
S2718
該MPEGデータをコンテンツ鍵k2で再暗号化
S2719
無線フレームを使い、SID＝αを付与して、暗号化されたMPEG映像を送出
S2720
無線ノード(のMPEGデコード／ディスプレイサブユニット)から認証先問い合わせ受信(SID＝α)
S2721
SID＝αの送信サブユニットを調査し、認証先応答として、「認証先は映像送信サブユニット」として、無線ノードに返答
S2722
映像送信サブユニット宛の認証要求の受信
S2723
Dの認証フォーマット(Dcert)を解く
S2724
無線ノードのMPEGデコード／ディスプレイサブユニットに対して、認証要求として、自ら(映像送信サブユニット)の認証フォーマットCcert等を送出
S2725
R21へ

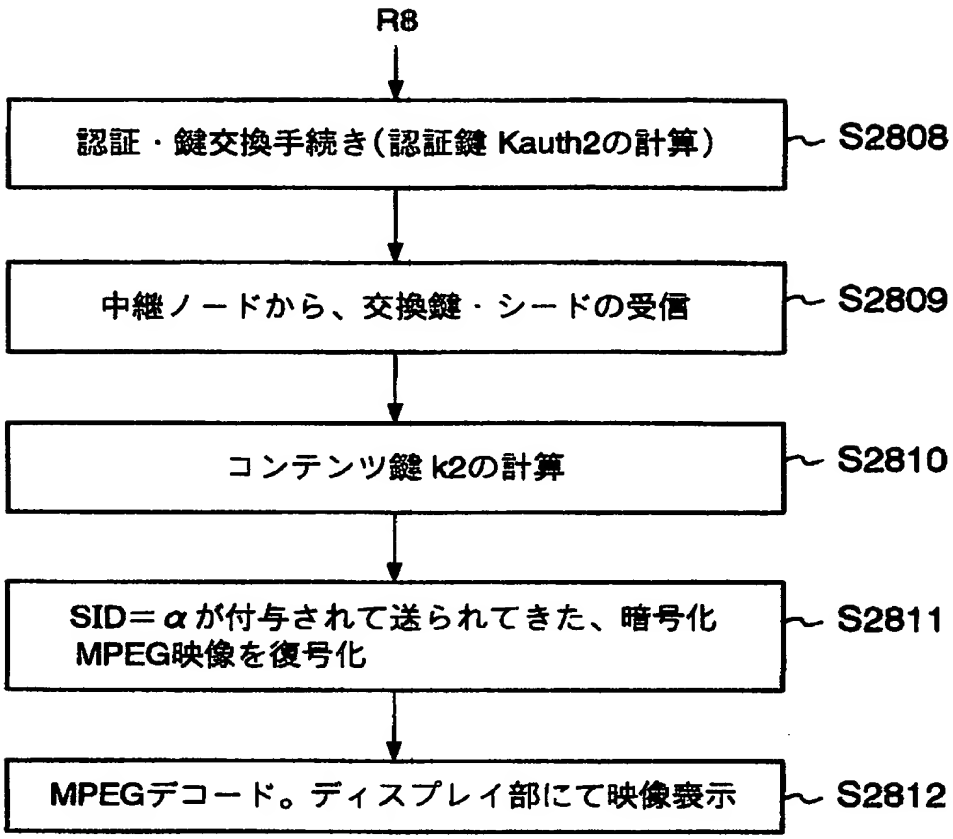
【図３１】


R21
認証・鍵交換手続き(認証鍵 kauth2の計算)
S2726
無線ノードに対し、交換鍵・シードの転送
S2727
MPEG映像をコンテンツ鍵 k2にて暗号化
S2728
SID＝αを付与して、暗号化されたMPEG映像を送出
S2729

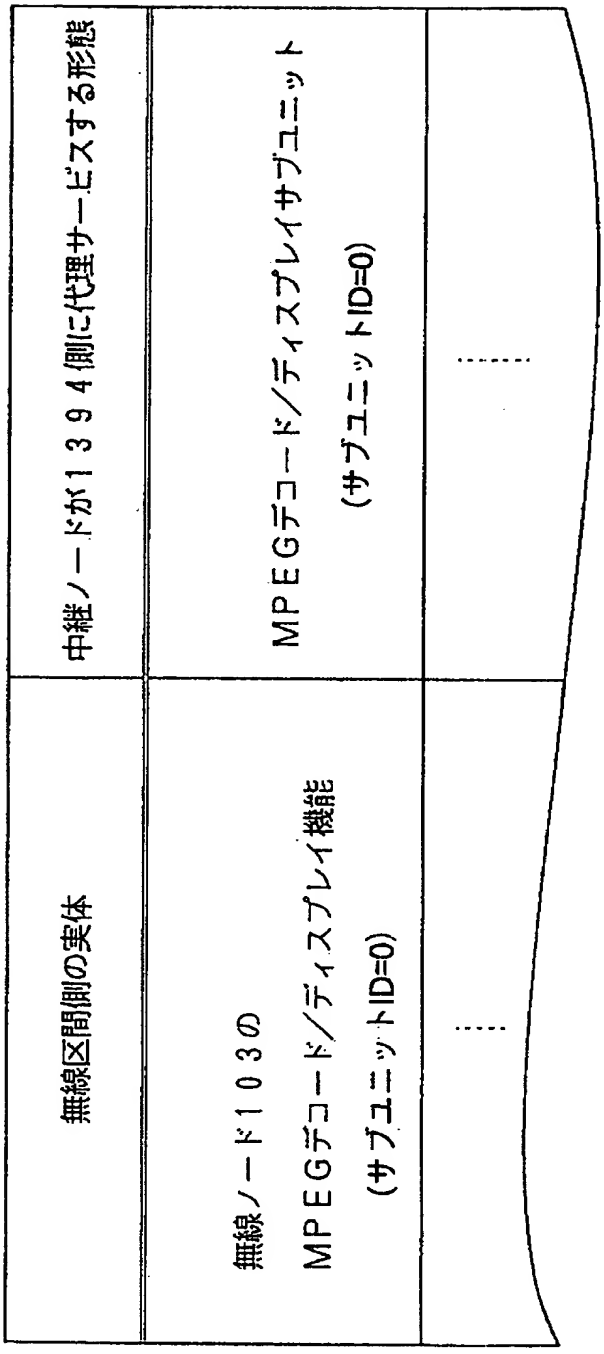
【図３２】


スタート
無線ノード構成情報の送信(MPEGデコード／ディスプレイサブユニットが存在することを通知。無線ノードが認証フォーマットを持つことを確認)
S2801
無線ノード制御パケットの受信
S2802
無線フレームを使い、SID＝αが付与された、暗号化されたMPEG映像を受信
S2803
MPEGデコード／ディスプレイサブユニットから、中継ノードに認証先問い合わせ送信(SID＝α)
S2804
認証先応答として、「認証先は映像送信サブユニット」との応答受信
S2805
映像送信サブユニット宛の認証要求の送信(認証フォーマットDcertを含める)
S2806
MPEGデコード／ディスプレイサブユニットに対して、中継ノードの映像送信サブユニットの認証フォーマットCcert等を含む認証要求を受信
S2807
R8へ

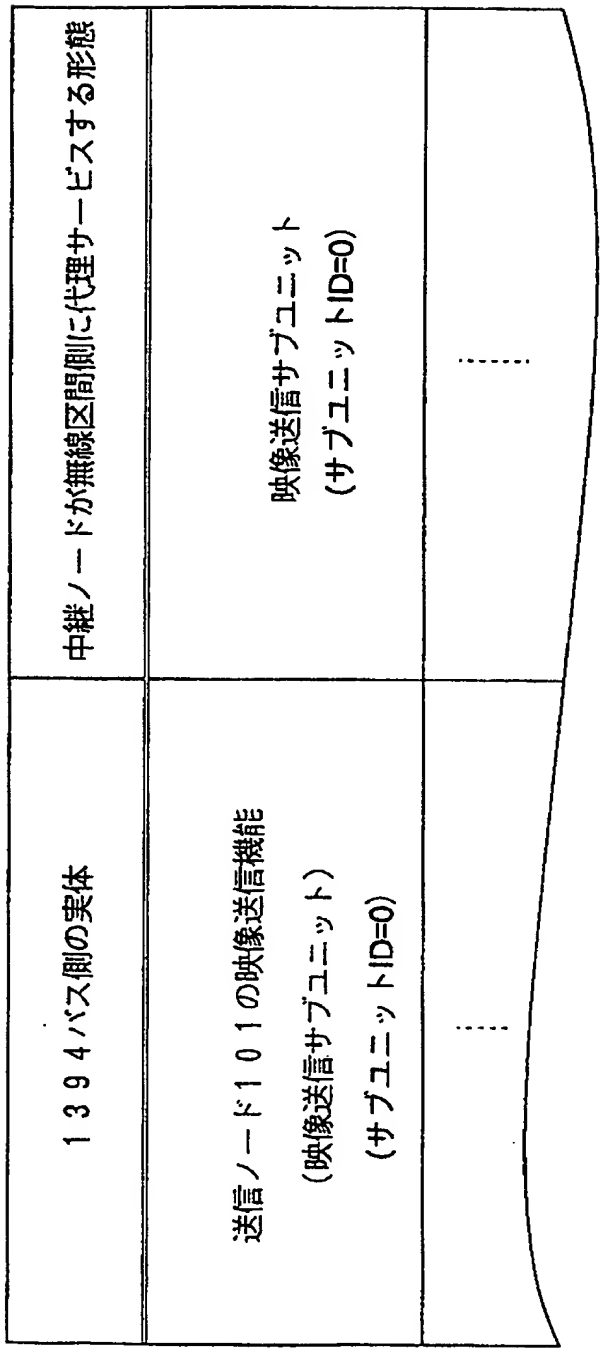
【図３３】


R8
認証・鍵交換手続き(認証鍵 Kauth2の計算)
S2808
中継ノードから、交換鍵・シードの受信
S2809
コンテンツ鍵 k2の計算
S2810
SID＝αが付与されて送られてきた、暗号化MPEG映像を復号化
S2811
MPEGデコード。ディスプレイ部にて映像表示
S2812

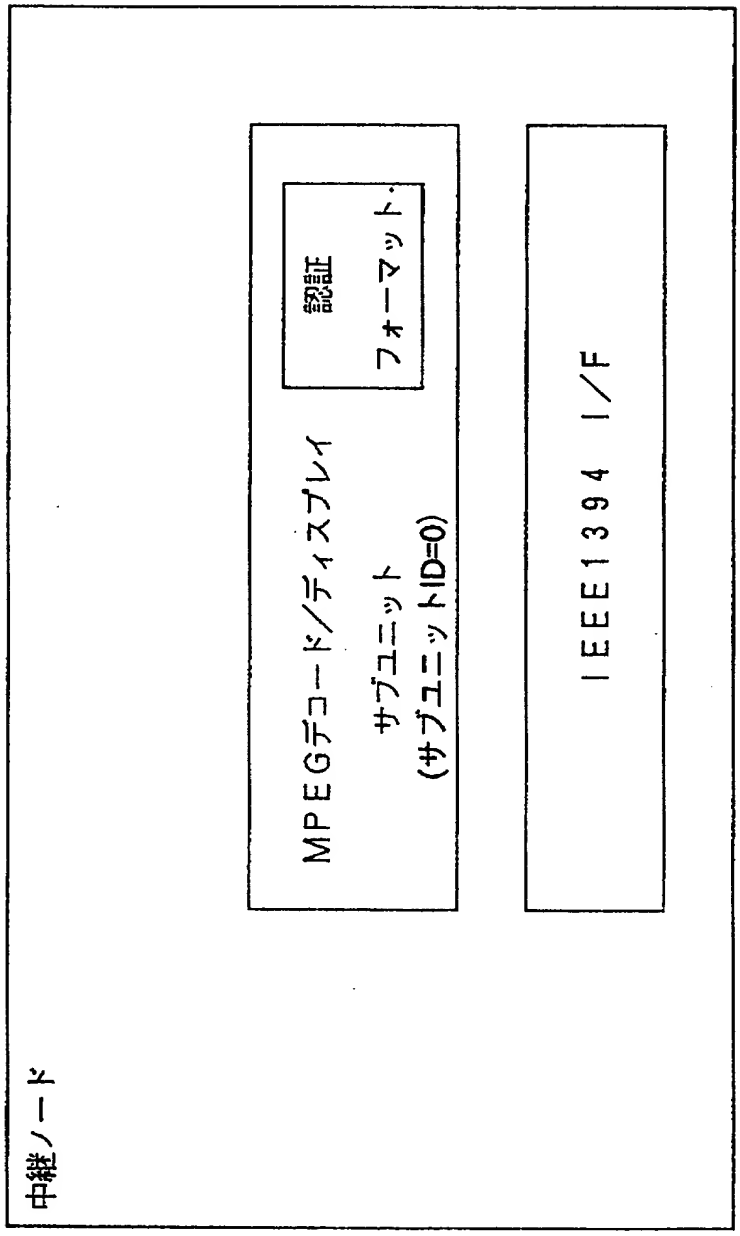
【図３４】


無線区間側の実体
中継ノードが１３９４側に代理サービスする形態
無線ノード１０３の
MPEGデコード／ディスプレイ機能
(サブユニットID=0)
MPEGデコード／ディスプレイサブユニット
(サブユニットID=0)

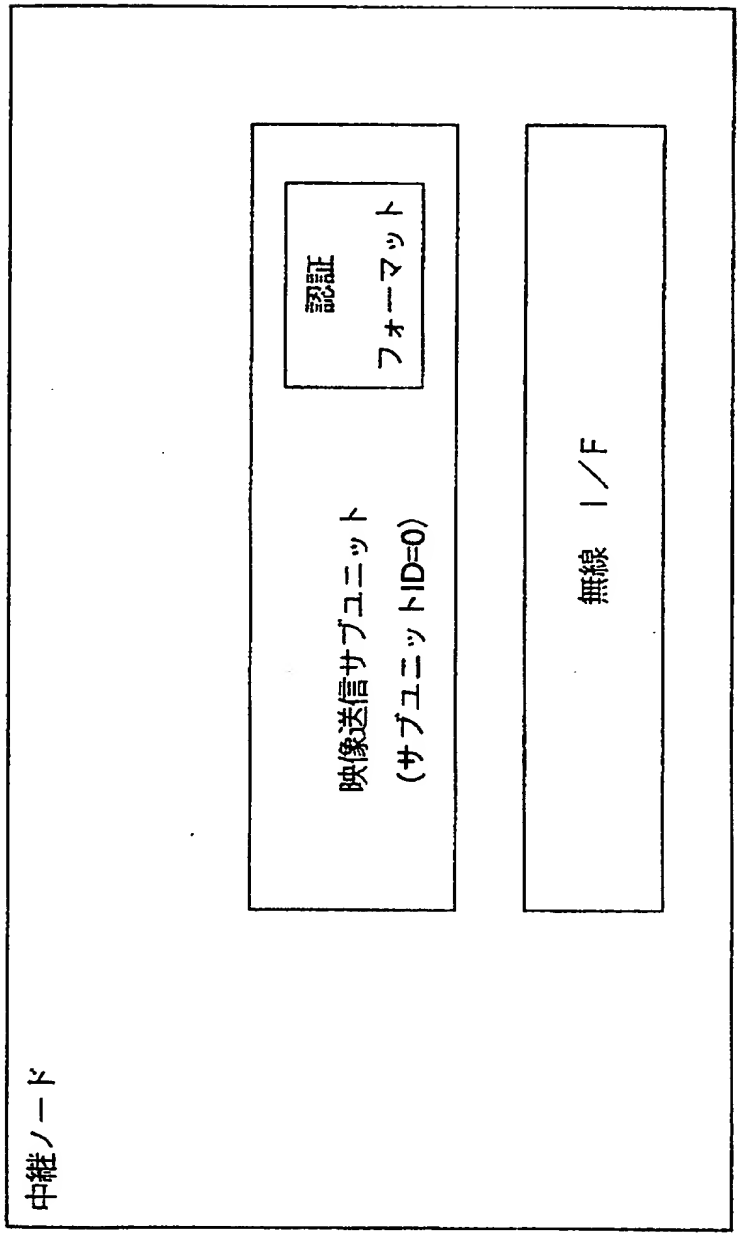
【図３５】


１３９４バス側の実体
中継ノードが無線区間側に代理サービスする形態
送信ノード１０１の映像送信機能
(映像送信サブユニット)
(サブユニットID=0)
映像送信サブユニット
(サブユニットID=0)

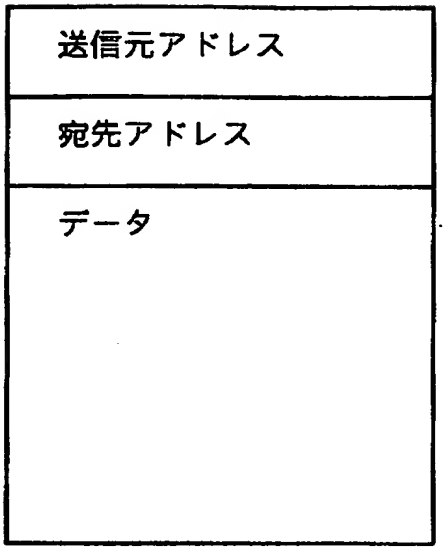
【図３６】


中継ノード
MPEGデコード／ディスプレイ
サブユニット
(サブユニットID=0)
認証
フォーマット
IEEE1394 I／F

【図３７】



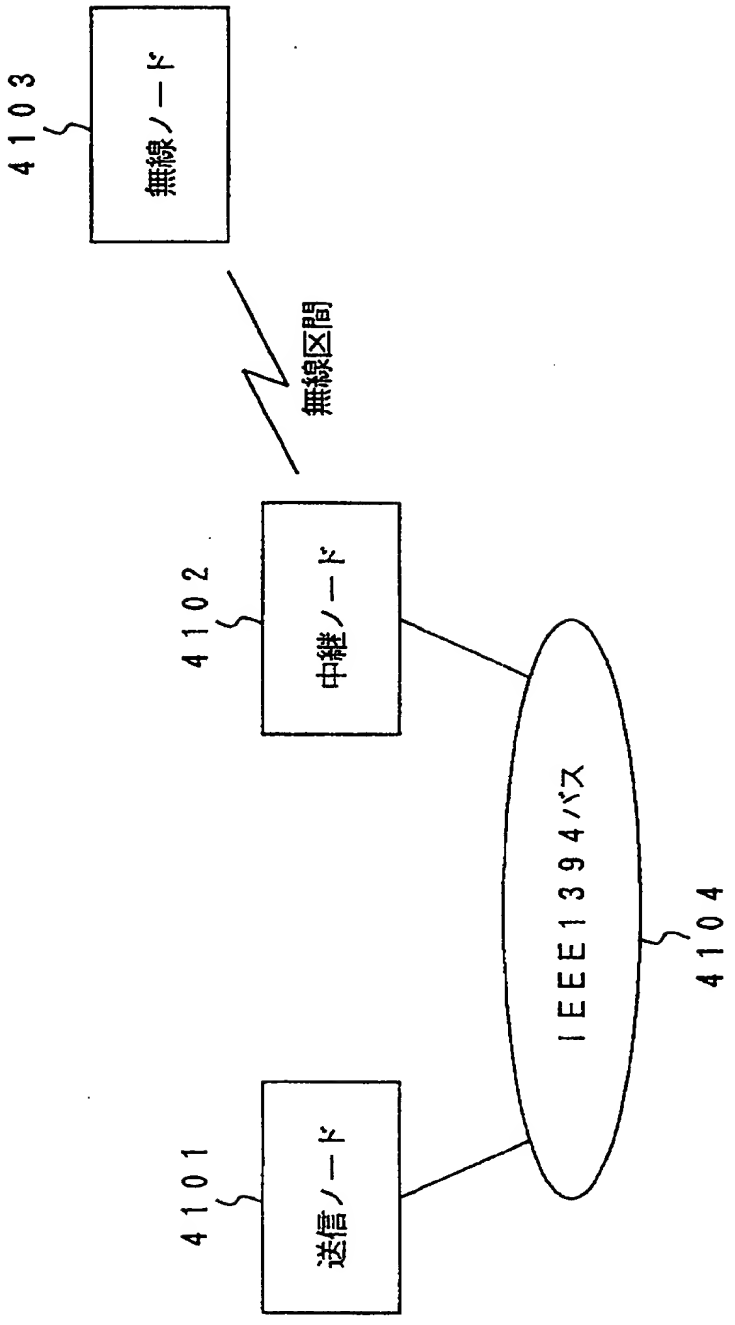
【図３８】



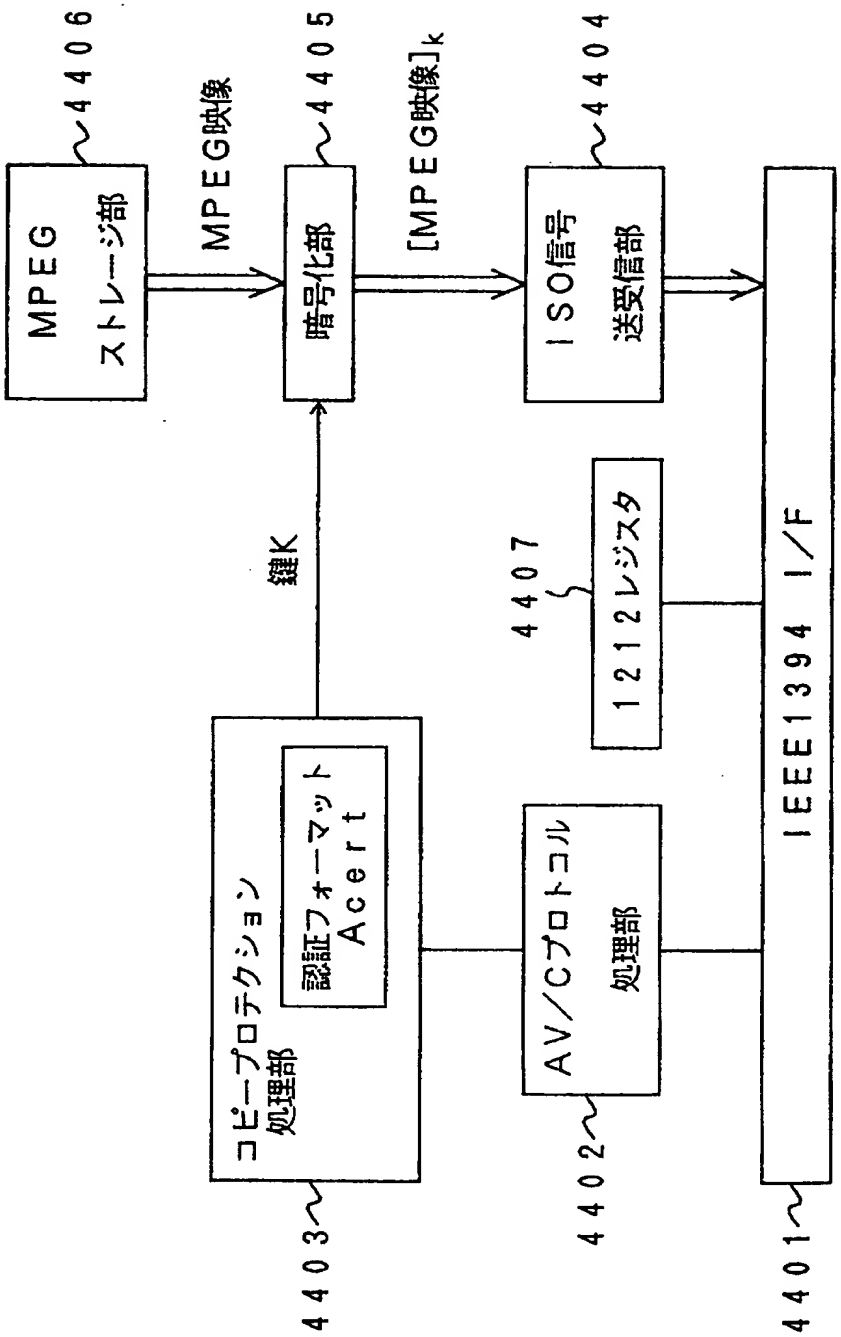
【図３９】

宛先ノード＝無線ノード
送信元ノード＝中継ノード
制御内容＝データ受信
使用SID＝α
データ送信先＝ MPEGデコード／ディスプレイ サブユニット(サブユニットID=0)
データ送信元＝ 映像送信サブユニット (サブユニットID=0)

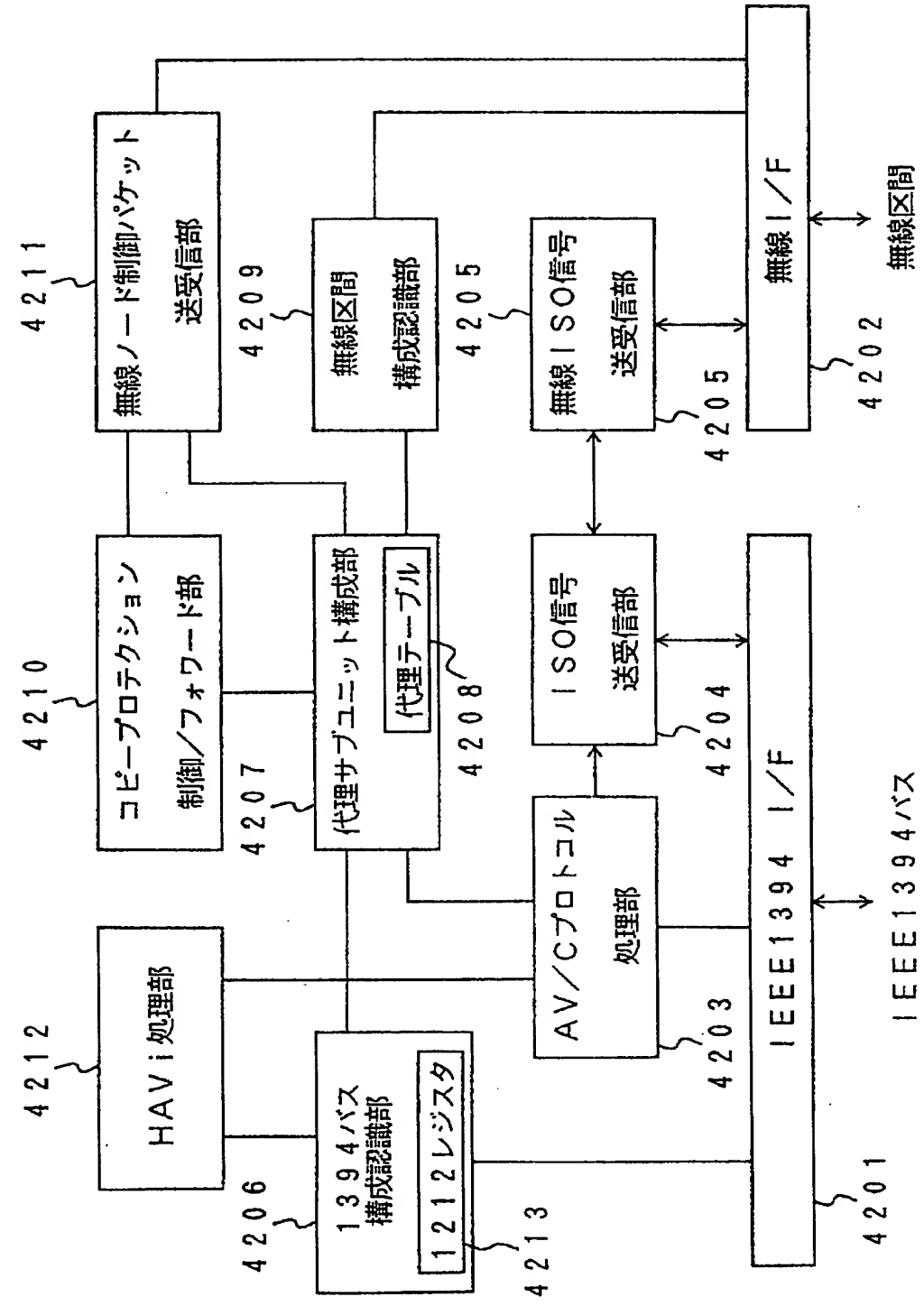
【図４０】



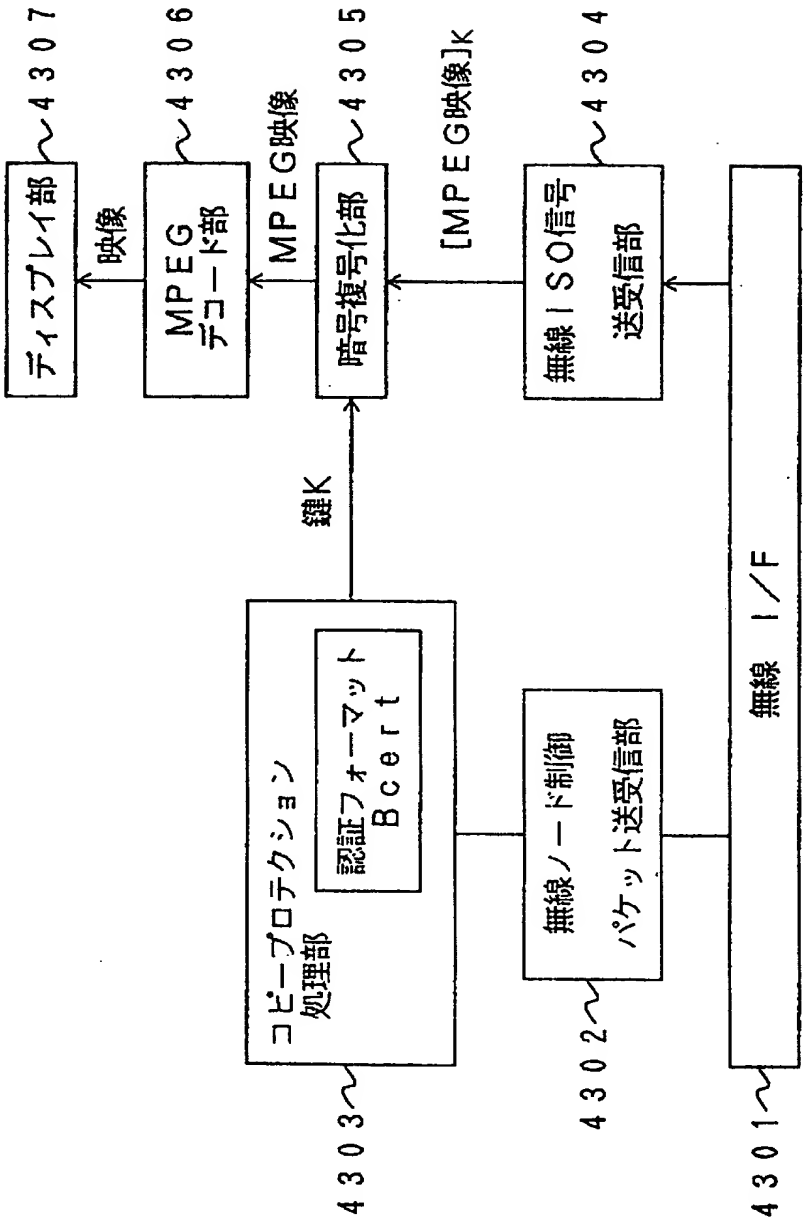
【図４１】


MPEG
ストレージ部
4406
MPEG映像
暗号化部
4405
[MPEG映像]k
ISO信号
送受信部
4404
鍵K
4407
1212レジスタ
コピープロテクション
処理部
認証フォーマット
Acert
AV／Cプロトコル
処理部
IEEE1394 I／F
4403
4402
4401

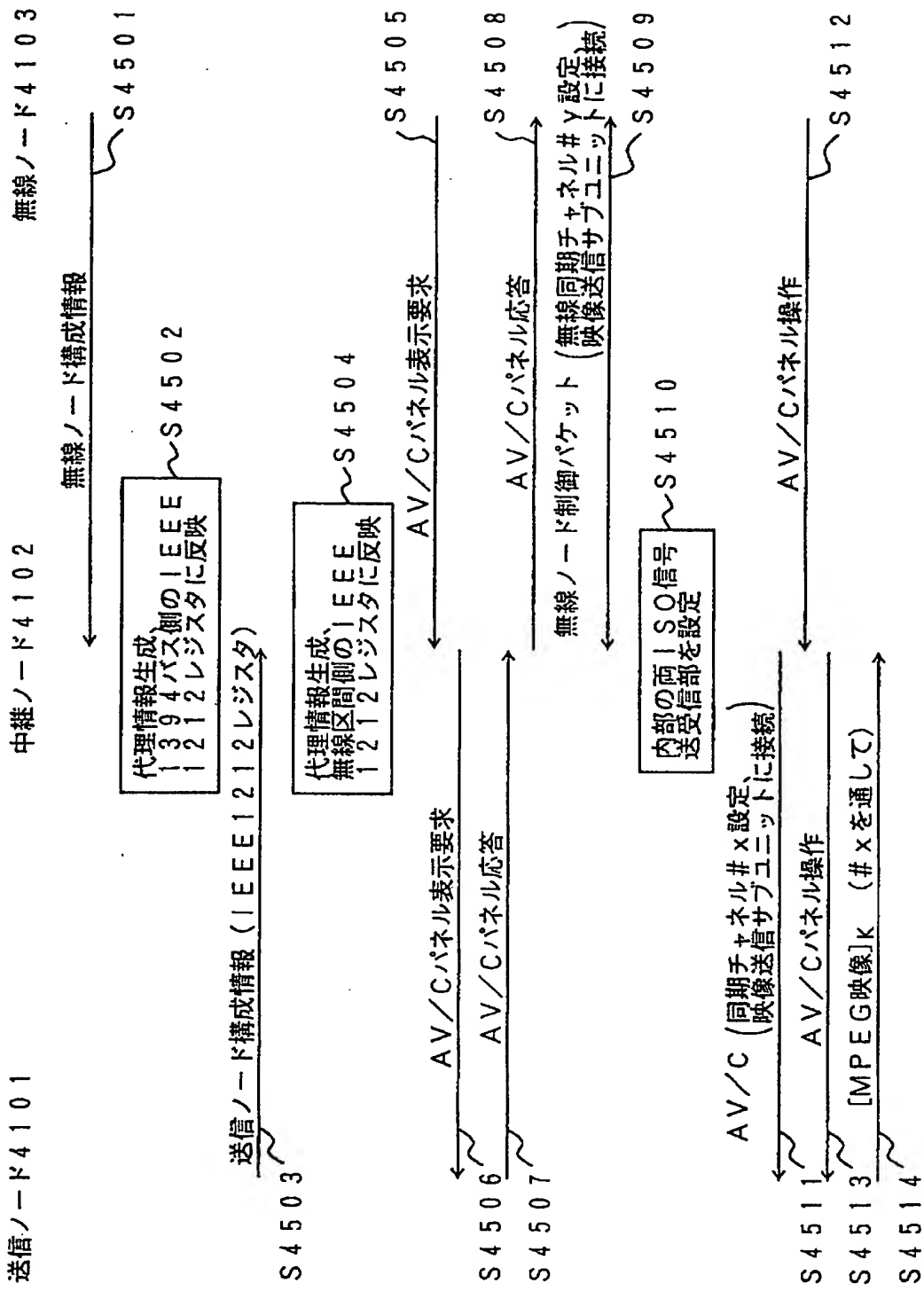
【図４２】


4211
無線ノード制御パケット送受信部
4209
無線区間構成認識部
4205
無線ISO信号送受信部
4205
無線I／F
4202
無線区間
4210
コピープロテクション制御／フォワード部
4207
代理サブユニット構成部
代理テーブル
4208
ISO信号送受信部
4204
4212
HAVi処理部
4206
1394バス構成認識部
1212レジスタ
4213
AV／Cプロトコル処理部
4203
IEEE1394 I／F
4201
IEEE1394バス

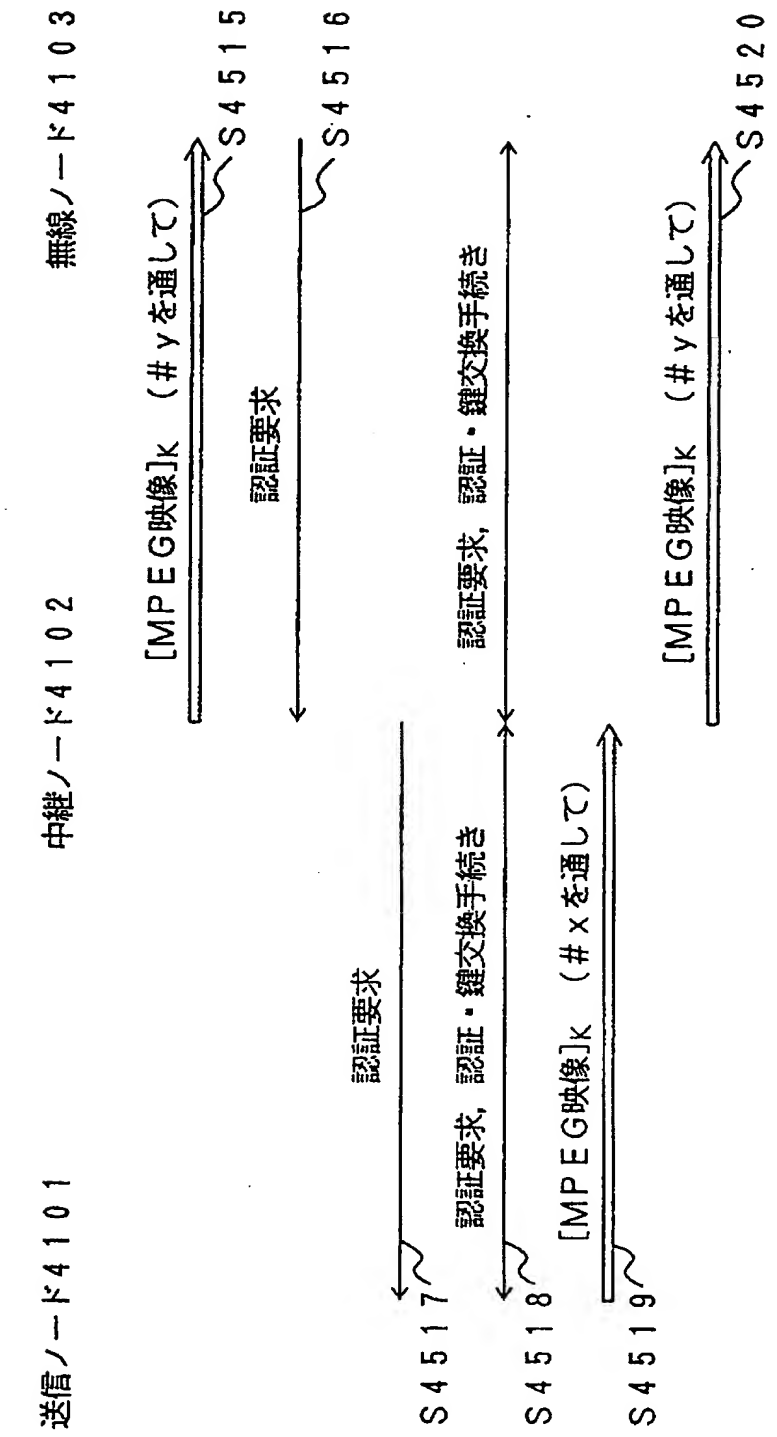
【図４３】


ディスプレイ部
4307
映像
MPEG
デコード部
4306
MPEG映像
暗号復号化部
4305
[MPEG映像]K
無線ISO信号
送受信部
4304
鍵K
コピープロテクション
処理部
認証フォーマット
Bcert
4303
無線ノード制御
パケット送受信部
4302
無線 I/F
4301

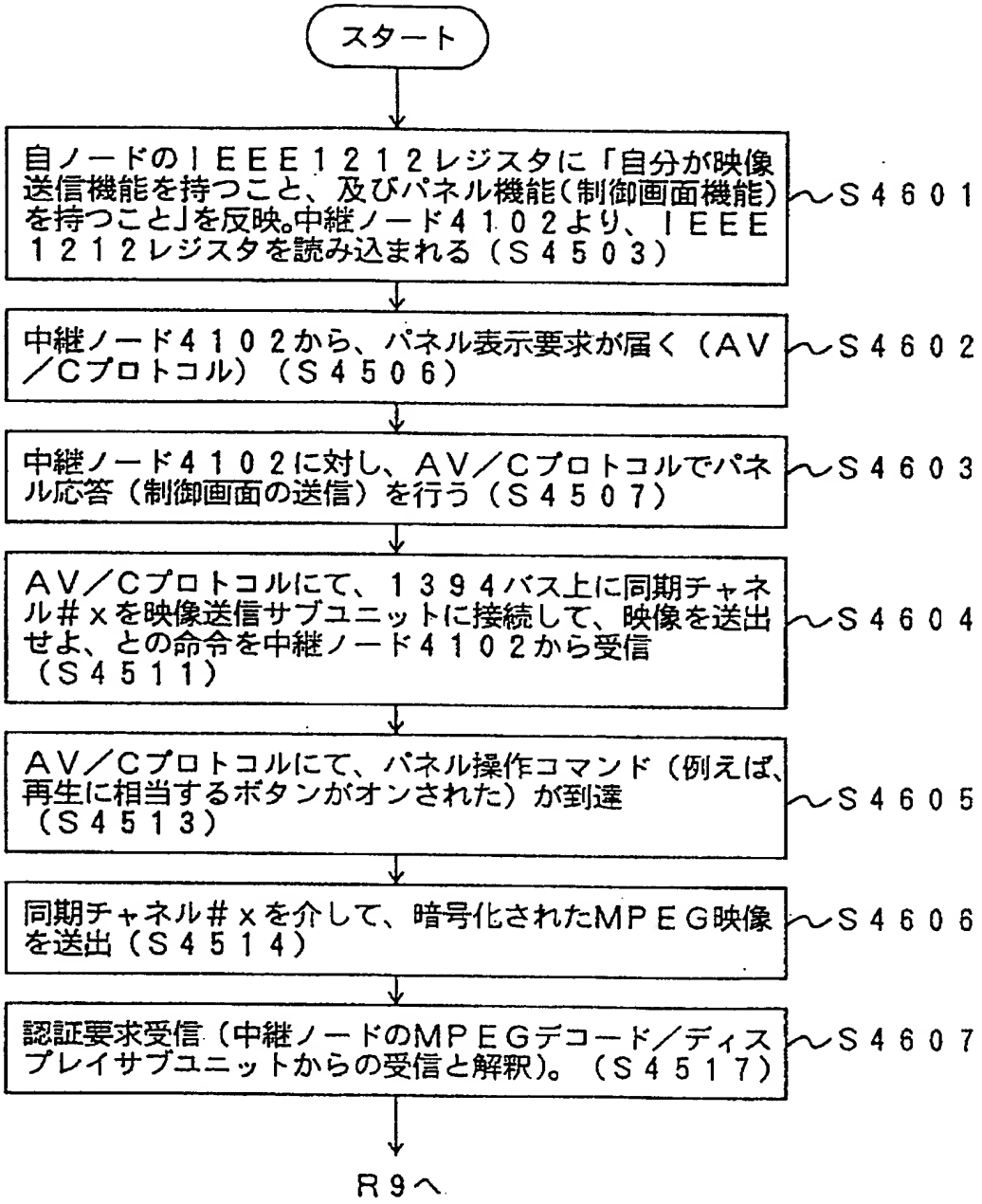
【図４４】


送信ノード４１０１
中継ノード４１０２
無線ノード４１０３
無線ノード構成情報
S４５０１
代理情報生成、
１３９４バス側のＩＥＥＥ
１２１２レジスタに反映
S４５０２
送信ノード構成情報（ＩＥＥＥ１２１２レジスタ）
S４５０３
代理情報生成、
無線区間側のＩＥＥＥ
１２１２レジスタに反映
S４５０４
AV／Cパネル表示要求
S４５０５
AV／Cパネル表示要求
S４５０６
AV／Cパネル応答
S４５０７
AV／Cパネル応答
S４５０８
無線ノード制御パケット（無線同期チャネル#Y設定、
映像送信サブユニットに接続）
S４５０９
内部の両ＩＳＯ信号
送受信部を設定
S４５１０
AV／C（同期チャネル#x設定、
映像送信サブユニットに接続）
S４５１１
AV／Cパネル操作
S４５１２
[MPEG映像]K（#xを通して）
S４５１３
AV／Cパネル操作
S４５１４

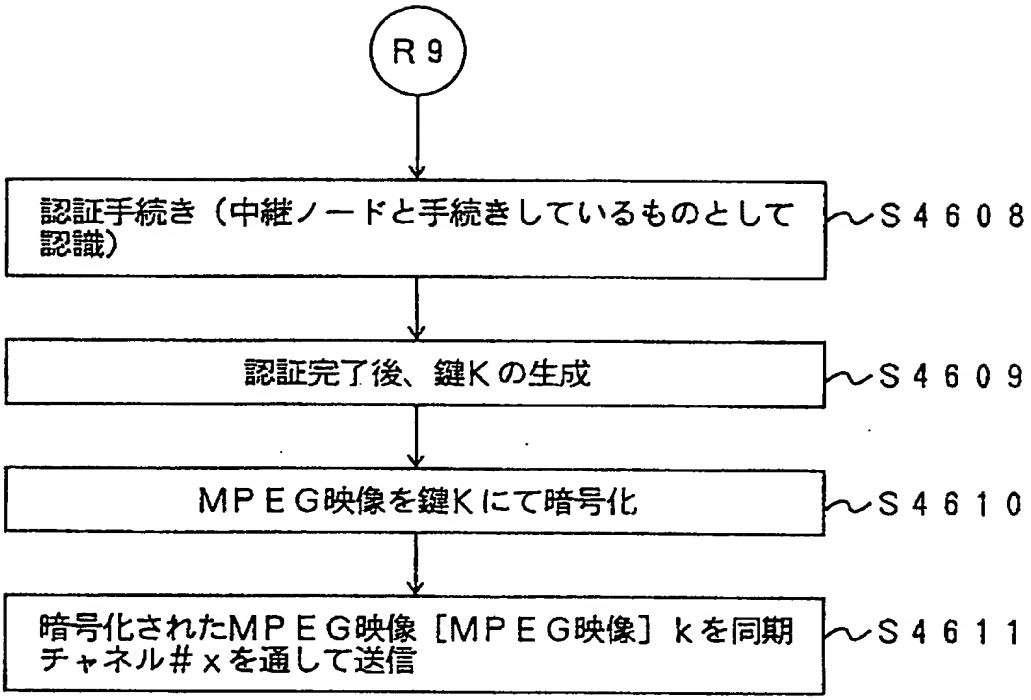
【図４５】


送信ノード４１０１
中継ノード４１０２
無線ノード４１０３
[MPEG映像]K （#yを通して）
S4515
認証要求
S4516
[MPEG映像]K （#yを通して）
S4520
認証要求
S4517
認証要求，認証・鍵交換手続き
認証要求，認証・鍵交換手続き
S4518
[MPEG映像]K （#xを通して）
S4519

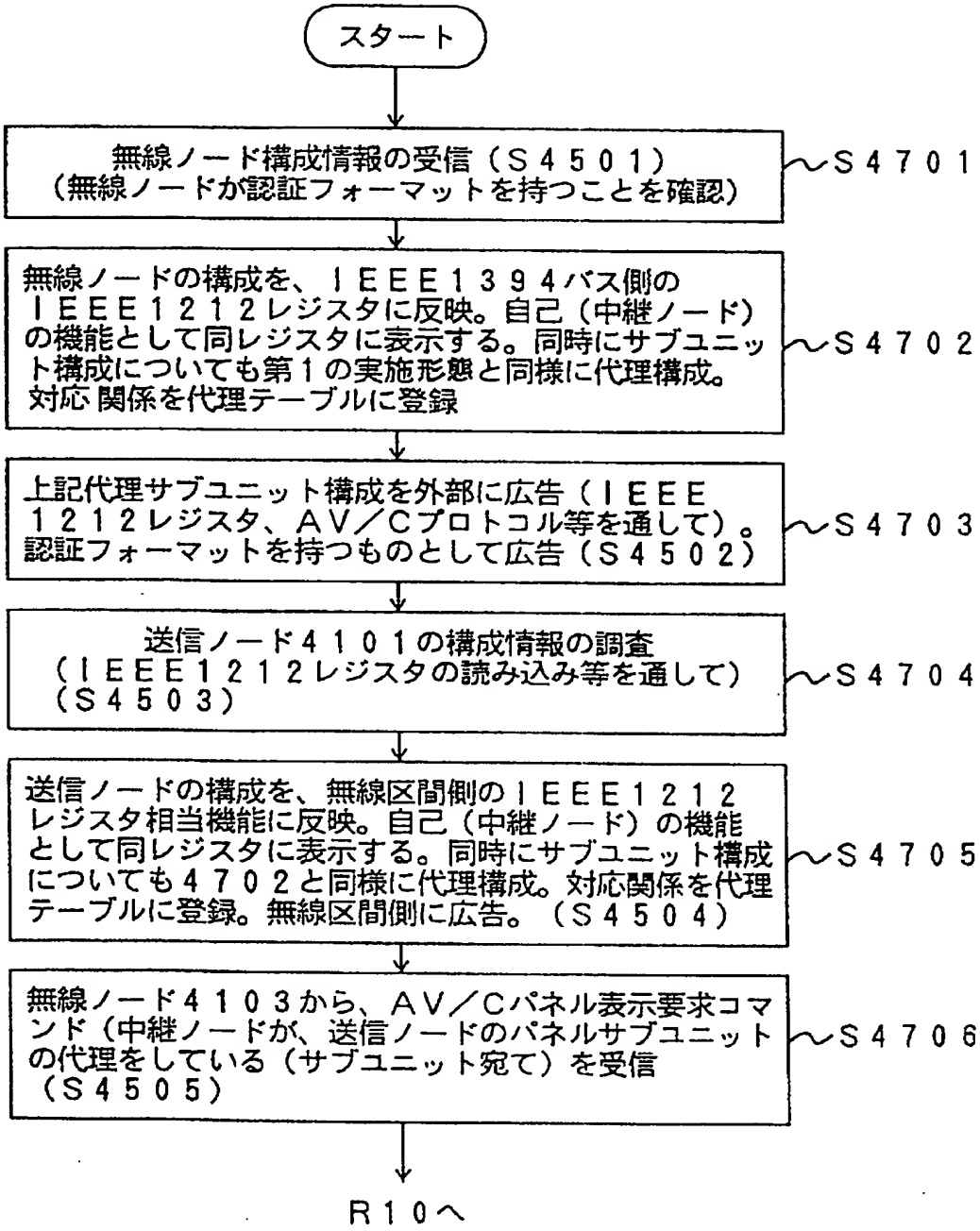
【図４６】


スタート
自ノードのＩＥＥＥ１２１２レジスタに「自分が映像送信機能を持つこと、及びパネル機能（制御画面機能）を持つこと」を反映。中継ノード４１０２より、ＩＥＥＥ１２１２レジスタを読み込まれる（Ｓ４５０３）
～Ｓ４６０１
中継ノード４１０２から、パネル表示要求が届く（ＡＶ／Ｃプロトコル）（Ｓ４５０６）
～Ｓ４６０２
中継ノード４１０２に対し、ＡＶ／Ｃプロトコルでパネル応答（制御画面の送信）を行う（Ｓ４５０７）
～Ｓ４６０３
ＡＶ／Ｃプロトコルにて、１３９４バス上に同期チャネル＃ｘを映像送信サブユニットに接続して、映像を送出せよ、との命令を中継ノード４１０２から受信（Ｓ４５１１）
～Ｓ４６０４
ＡＶ／Ｃプロトコルにて、パネル操作コマンド（例えば、再生に相当するボタンがオンされた）が到達（Ｓ４５１３）
～Ｓ４６０５
同期チャネル＃ｘを介して、暗号化されたＭＰＥＧ映像を送出（Ｓ４５１４）
～Ｓ４６０６
認証要求受信（中継ノードのＭＰＥＧデコード／ディスプレイサブユニットからの受信と解釈）。（Ｓ４５１７）
～Ｓ４６０７
Ｒ９へ

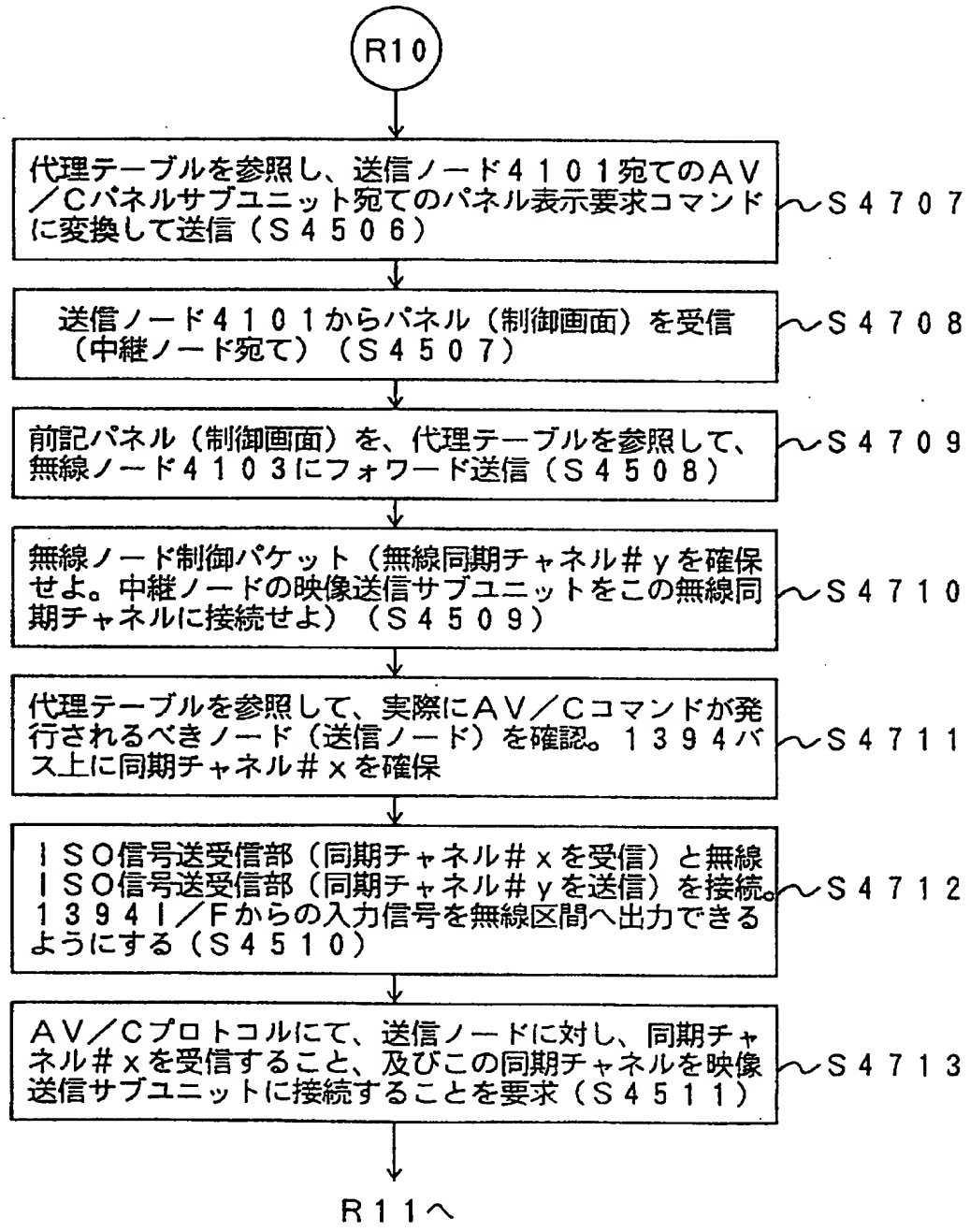
【図４７】


R9
認証手続き（中継ノードと手続きしているものとして認識）
S４６０８
認証完了後、鍵Kの生成
S４６０９
MPEG映像を鍵Kにて暗号化
S４６１０
暗号化されたMPEG映像［MPEG映像］kを同期チャネル#xを通して送信
S４６１１

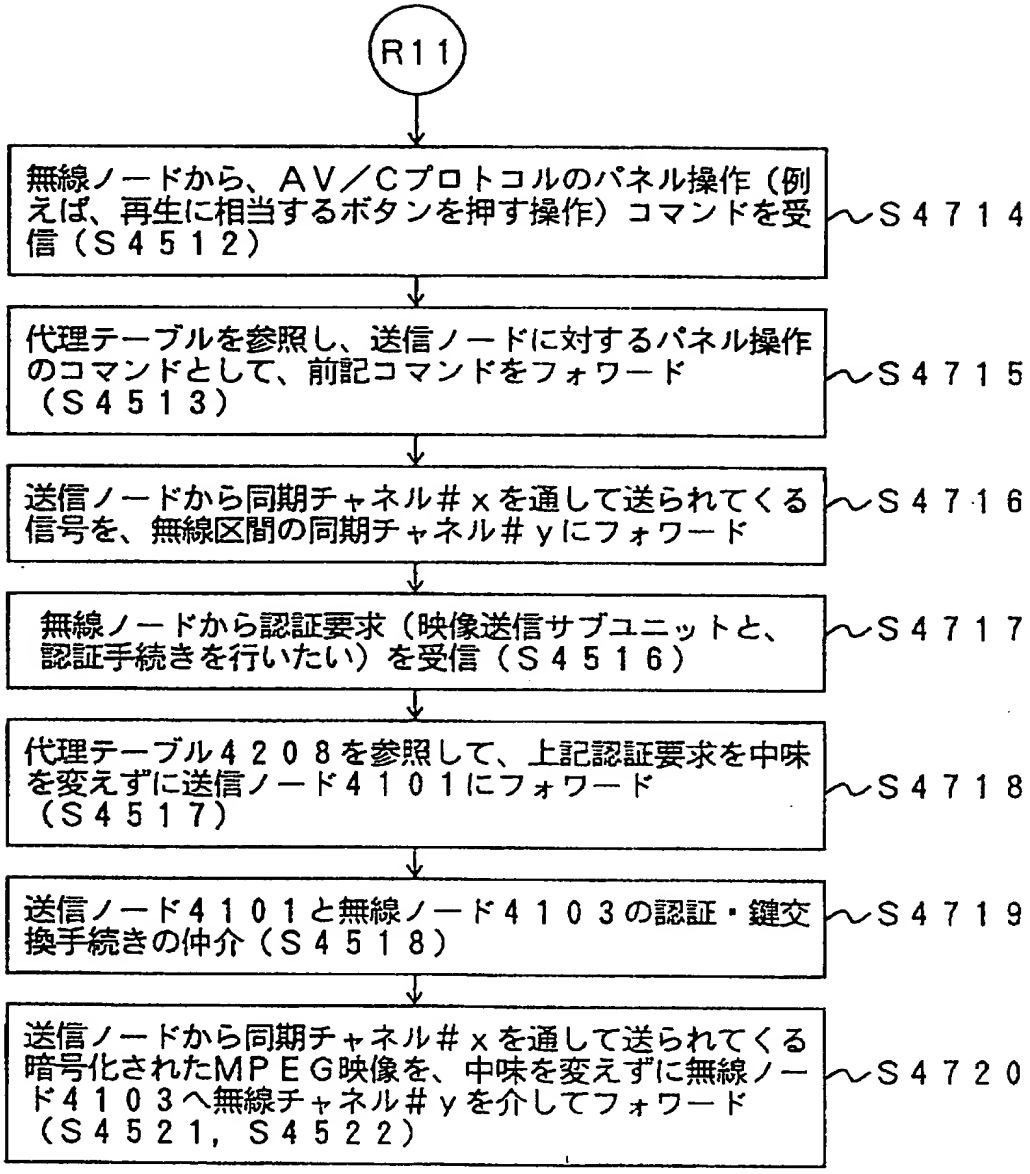
【図４８】


スタート
無線ノード構成情報の受信（Ｓ４５０１）
（無線ノードが認証フォーマットを持つことを確認）
～Ｓ４７０１
無線ノードの構成を、ＩＥＥＥ１３９４バス側のＩＥＥＥ１２１２レジスタに反映。自己（中継ノード）の機能として同レジスタに表示する。同時にサブユニット構成についても第１の実施形態と同様に代理構成。対応関係を代理テーブルに登録
～Ｓ４７０２
上記代理サブユニット構成を外部に広告（ＩＥＥＥ１２１２レジスタ、ＡＶ／Ｃプロトコル等を通して）。認証フォーマットを持つものとして広告（Ｓ４５０２）
～Ｓ４７０３
送信ノード４１０１の構成情報の調査
（ＩＥＥＥ１２１２レジスタの読み込み等を通して）
（Ｓ４５０３）
～Ｓ４７０４
送信ノードの構成を、無線区間側のＩＥＥＥ１２１２レジスタ相当機能に反映。自己（中継ノード）の機能として同レジスタに表示する。同時にサブユニット構成についても４７０２と同様に代理構成。対応関係を代理テーブルに登録。無線区間側に広告。（Ｓ４５０４）
～Ｓ４７０５
無線ノード４１０３から、ＡＶ／Ｃパネル表示要求コマンド（中継ノードが、送信ノードのパネルサブユニットの代理をしている（サブユニット宛て）を受信
（Ｓ４５０５）
～Ｓ４７０６
Ｒ１０へ

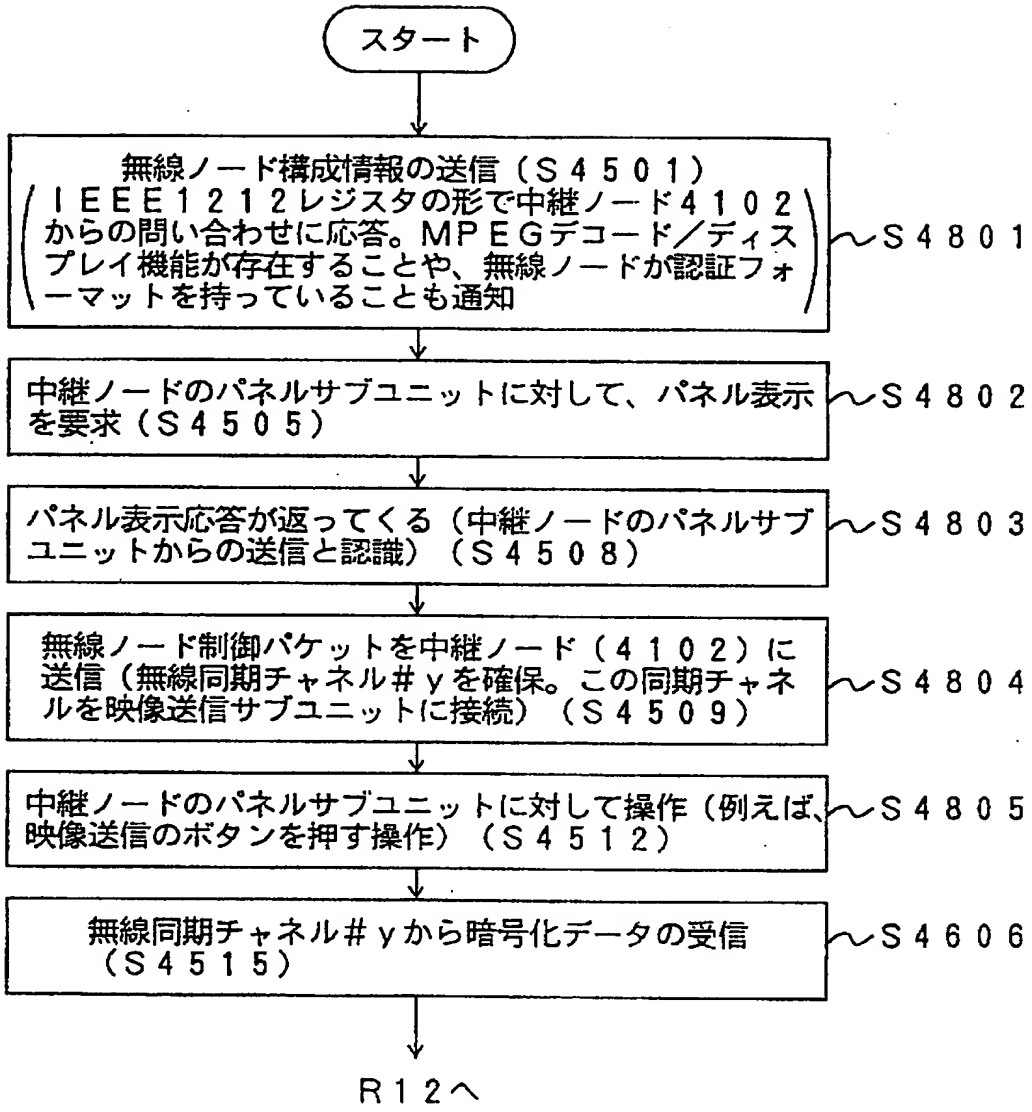
【図４９】


R10
代理テーブルを参照し、送信ノード４１０１宛てのＡＶ／Ｃパネルサブユニット宛てのパネル表示要求コマンドに変換して送信（Ｓ４５０６）
Ｓ４７０７
送信ノード４１０１からパネル（制御画面）を受信（中継ノード宛て）（Ｓ４５０７）
Ｓ４７０８
前記パネル（制御画面）を、代理テーブルを参照して、無線ノード４１０３にフォワード送信（Ｓ４５０８）
Ｓ４７０９
無線ノード制御パケット（無線同期チャネル＃ｙを確保せよ。中継ノードの映像送信サブユニットをこの無線同期チャネルに接続せよ）（Ｓ４５０９）
Ｓ４７１０
代理テーブルを参照して、実際にＡＶ／Ｃコマンドが発行されるべきノード（送信ノード）を確認。１３９４バス上に同期チャネル＃ｘを確保
Ｓ４７１１
ＩＳＯ信号送受信部（同期チャネル＃ｘを受信）と無線ＩＳＯ信号送受信部（同期チャネル＃ｙを送信）を接続。１３９４Ｉ／Ｆからの入力信号を無線区間へ出力できるようにする（Ｓ４５１０）
Ｓ４７１２
ＡＶ／Ｃプロトコルにて、送信ノードに対し、同期チャネル＃ｘを受信すること、及びこの同期チャネルを映像送信サブユニットに接続することを要求（Ｓ４５１１）
Ｓ４７１３
R11へ

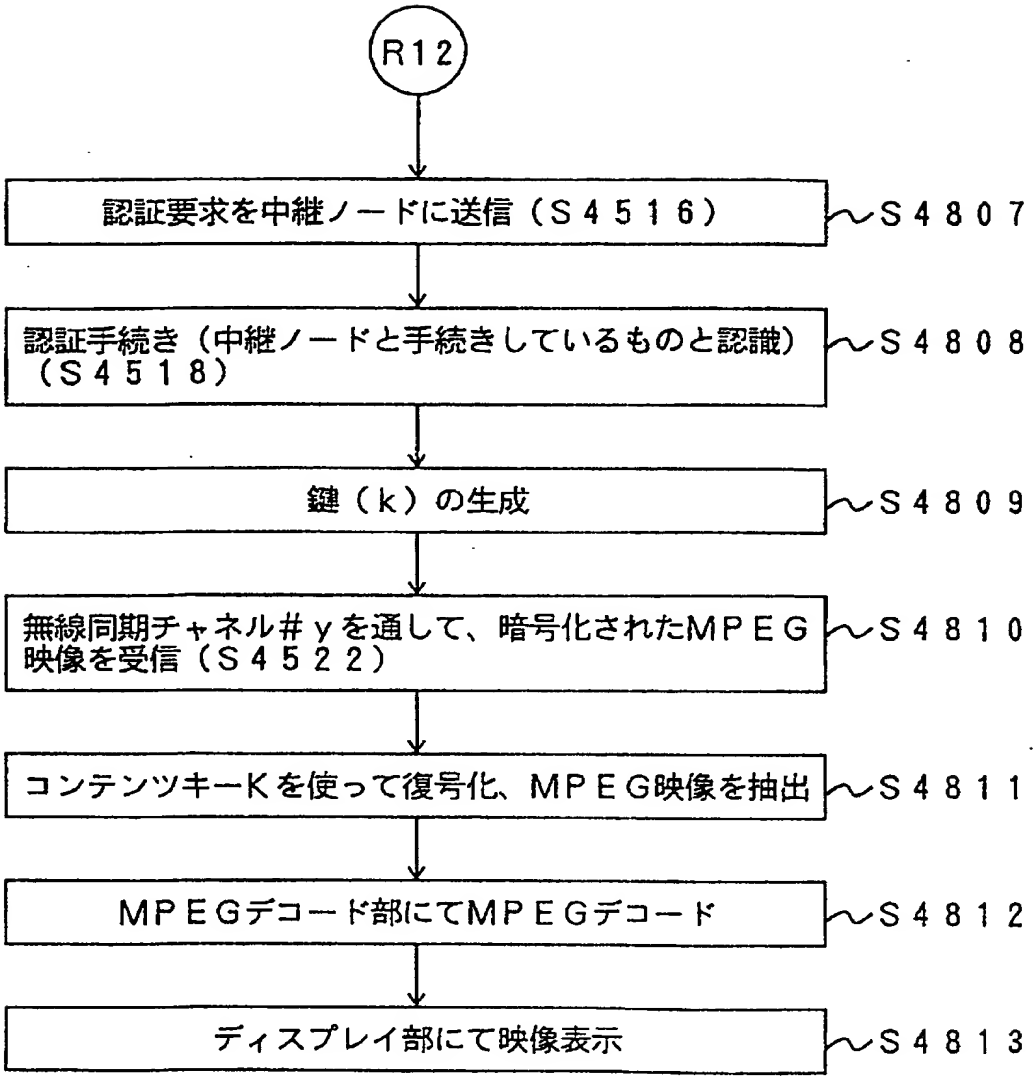
【図５０】


R11
無線ノードから、ＡＶ／Ｃプロトコルのパネル操作（例えば、再生に相当するボタンを押す操作）コマンドを受信（Ｓ４５１２）
Ｓ４７１４
代理テーブルを参照し、送信ノードに対するパネル操作のコマンドとして、前記コマンドをフォワード（Ｓ４５１３）
Ｓ４７１５
送信ノードから同期チャネル＃ｘを通して送られてくる信号を、無線区間の同期チャネル＃ｙにフォワード
Ｓ４７１６
無線ノードから認証要求（映像送信サブユニットと、認証手続きを行いたい）を受信（Ｓ４５１６）
Ｓ４７１７
代理テーブル４２０８を参照して、上記認証要求を中味を変えずに送信ノード４１０１にフォワード（Ｓ４５１７）
Ｓ４７１８
送信ノード４１０１と無線ノード４１０３の認証・鍵交換手続きの仲介（Ｓ４５１８）
Ｓ４７１９
送信ノードから同期チャネル＃ｘを通して送られてくる暗号化されたＭＰＥＧ映像を、中味を変えずに無線ノード４１０３へ無線チャネル＃ｙを介してフォワード（Ｓ４５２１，Ｓ４５２２）
Ｓ４７２０

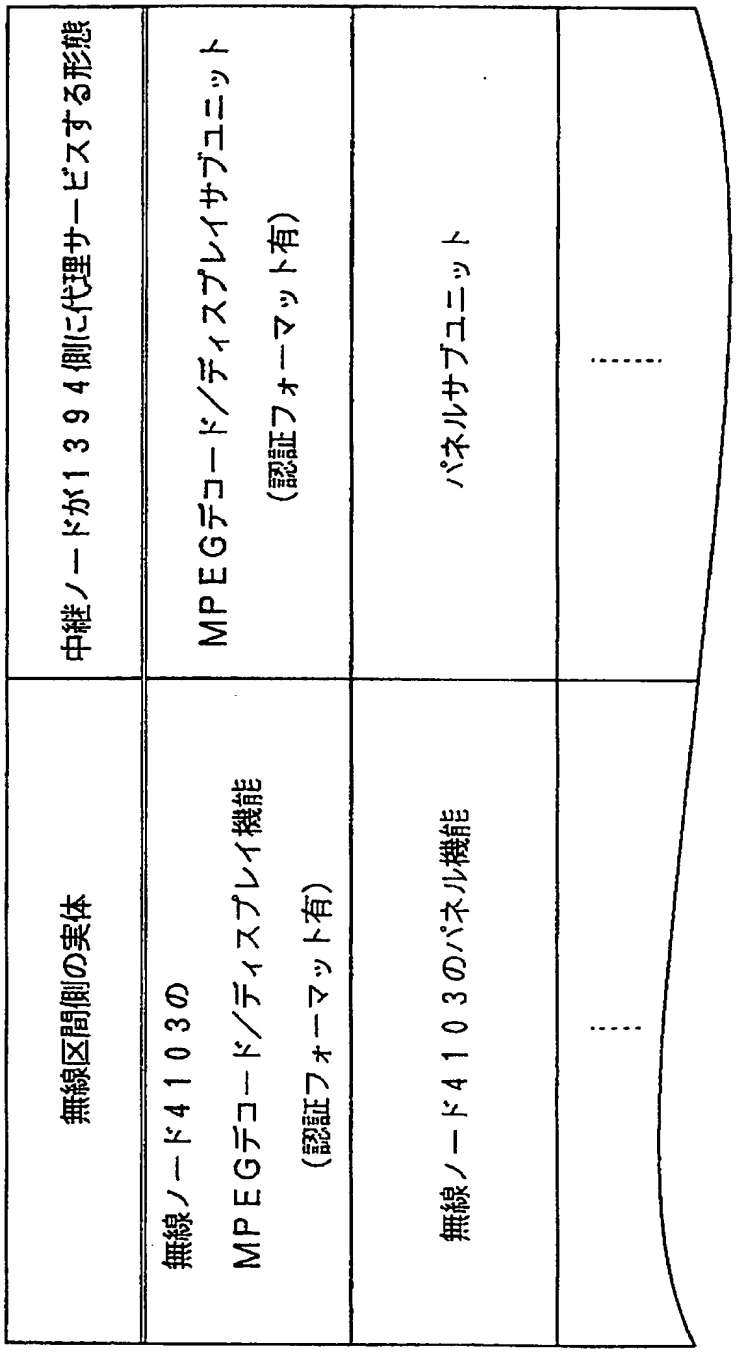
【図５１】


スタート
無線ノード構成情報の送信（Ｓ４５０１）
（ＩＥＥＥ１２１２レジスタの形で中継ノード４１０２からの問い合わせに応答。ＭＰＥＧデコード／ディスプレイ機能が存在することや、無線ノードが認証フォーマットを持っていることも通知）
～Ｓ４８０１
中継ノードのパネルサブユニットに対して、パネル表示を要求（Ｓ４５０５）
～Ｓ４８０２
パネル表示応答が返ってくる（中継ノードのパネルサブユニットからの送信と認識）（Ｓ４５０８）
～Ｓ４８０３
無線ノード制御パケットを中継ノード（４１０２）に送信（無線同期チャネル＃ｙを確保。この同期チャネルを映像送信サブユニットに接続）（Ｓ４５０９）
～Ｓ４８０４
中継ノードのパネルサブユニットに対して操作（例えば、映像送信のボタンを押す操作）（Ｓ４５１２）
～Ｓ４８０５
無線同期チャネル＃ｙから暗号化データの受信（Ｓ４５１５）
～Ｓ４６０６
Ｒ１２へ

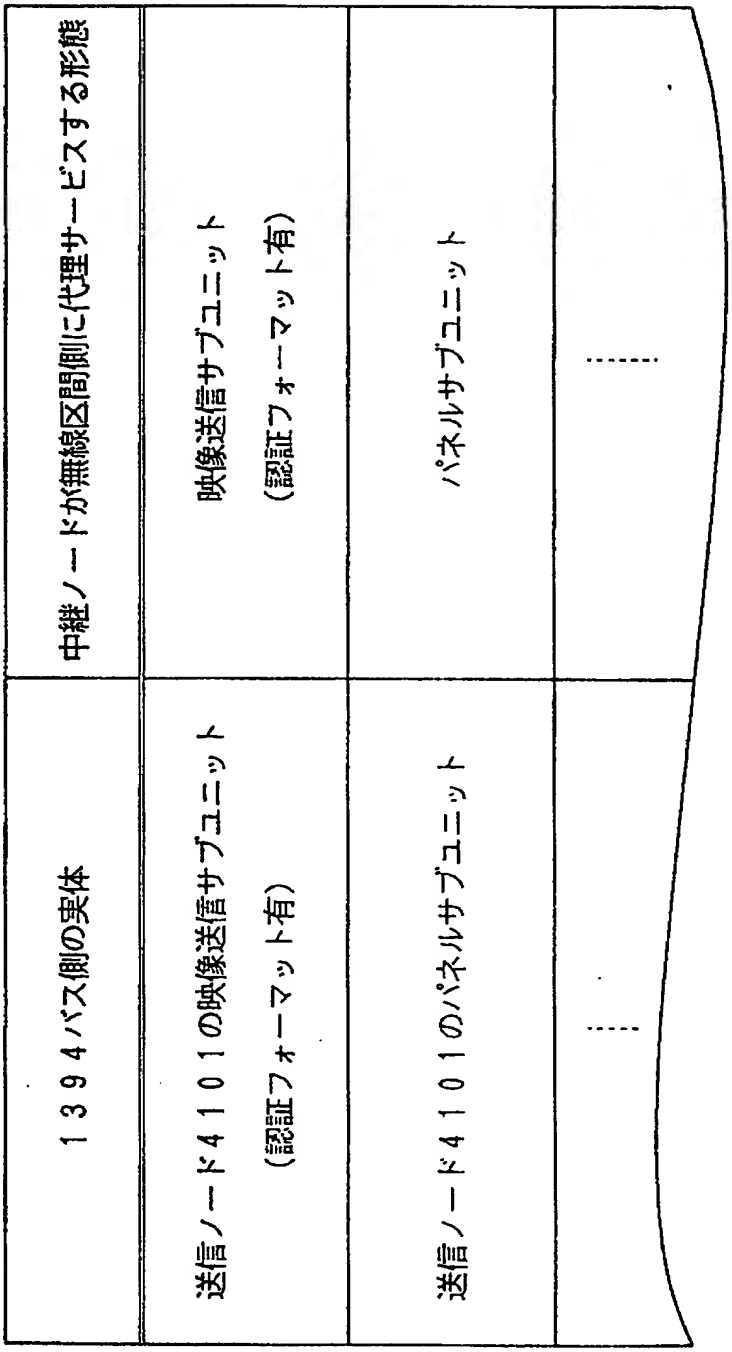
【図５２】


R12
認証要求を中継ノードに送信（Ｓ４５１６）
Ｓ４８０７
認証手続き（中継ノードと手続きしているものと認識）（Ｓ４５１８）
Ｓ４８０８
鍵（ｋ）の生成
Ｓ４８０９
無線同期チャネル＃ｙを通して、暗号化されたＭＰＥＧ映像を受信（Ｓ４５２２）
Ｓ４８１０
コンテンツキーＫを使って復号化、ＭＰＥＧ映像を抽出
Ｓ４８１１
ＭＰＥＧデコード部にてＭＰＥＧデコード
Ｓ４８１２
ディスプレイ部にて映像表示
Ｓ４８１３

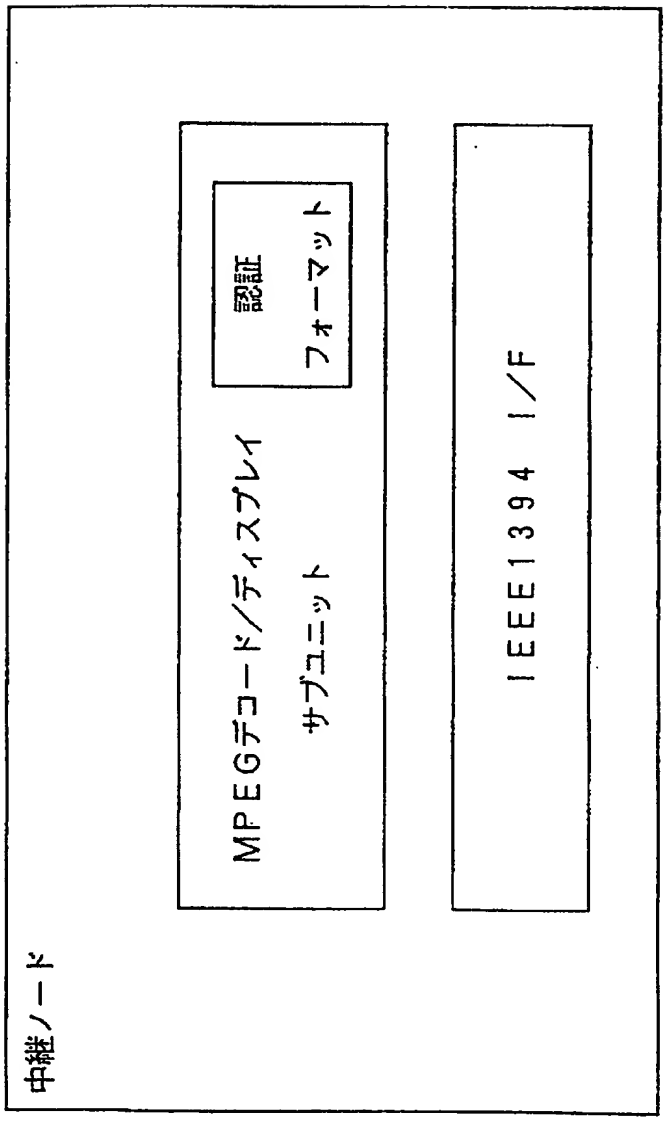
【図５３】


無線区間側の実体
中継ノードが１３９４側に代理サービスする形態
無線ノード４１０３の
ＭＰＥＧデコード／ディスプレイ機能
（認証フォーマット有）
ＭＰＥＧデコード／ディスプレイサブユニット
（認証フォーマット有）
無線ノード４１０３のパネル機能
パネルサブユニット
・・・・
・・・・・

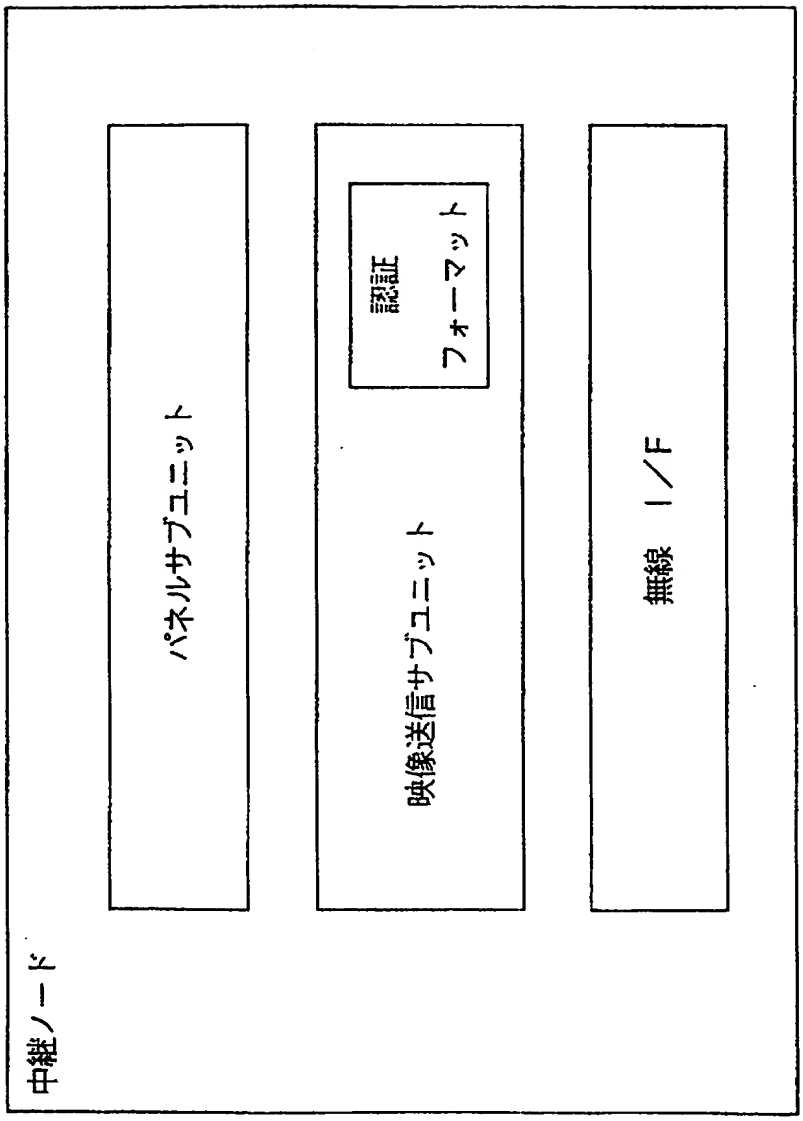
【図５４】


１３９４バス側の実体
中継ノードが無線区間側に代理サービスする形態
送信ノード４１０１の映像送信サブユニット
（認証フォーマット有）
映像送信サブユニット
（認証フォーマット有）
送信ノード４１０１のパネルサブユニット
パネルサブユニット

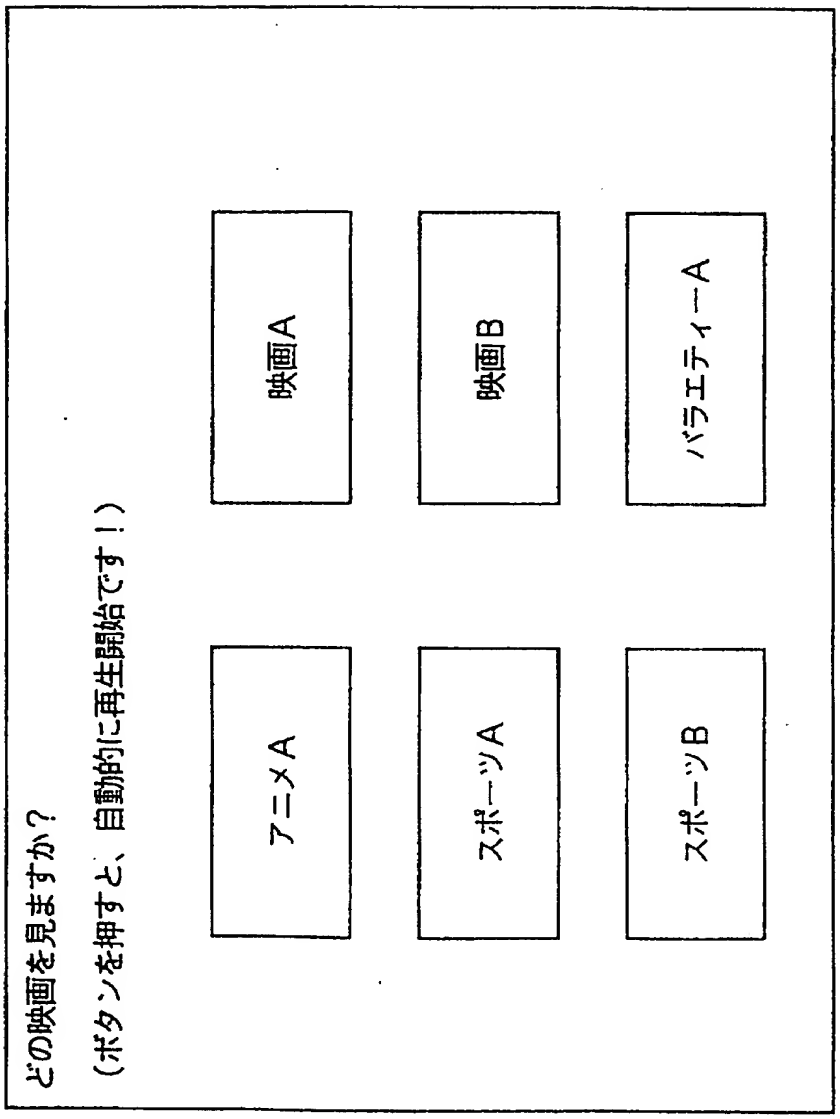
【図５５】



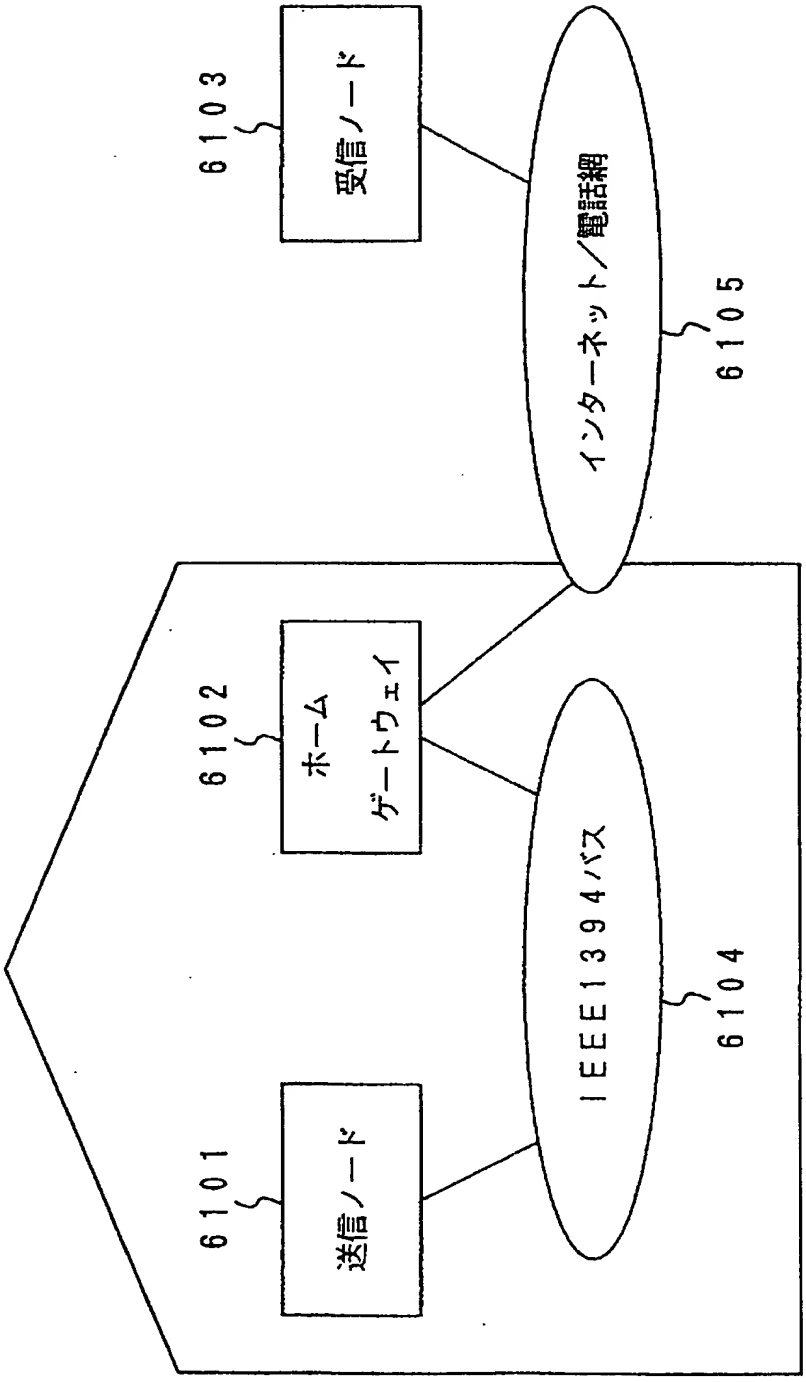
【図５６】



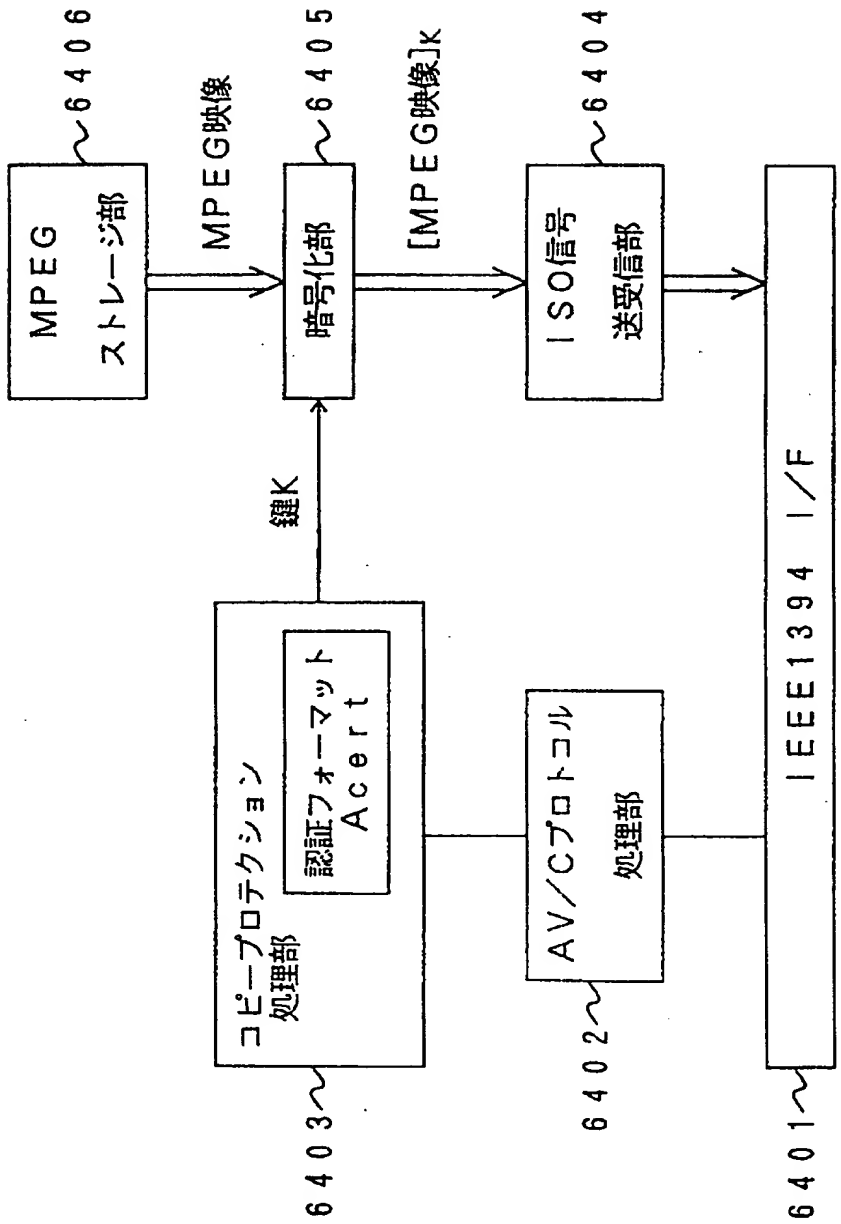
【図５７】


どの映画を見ますか？
（ボタンを押すと、自動的に再生開始です！）
映画A
映画B
バラエティーA
アニメA
スポーツA
スポーツB

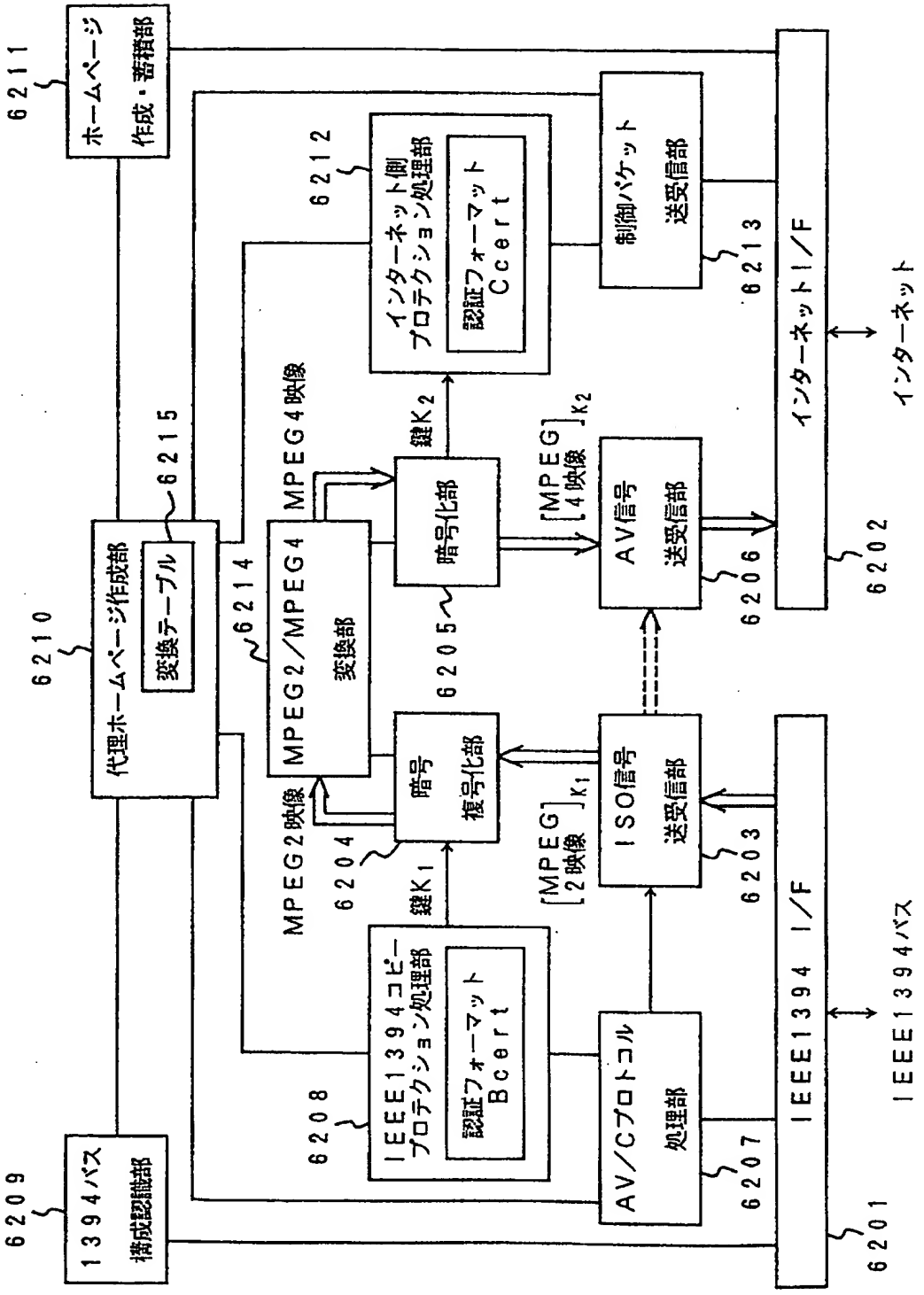
【図５８】


6103
受信ノード
インターネット／電話網
6105
6102
ホーム
ゲートウェイ
IEEE1394バス
6104
6101
送信ノード

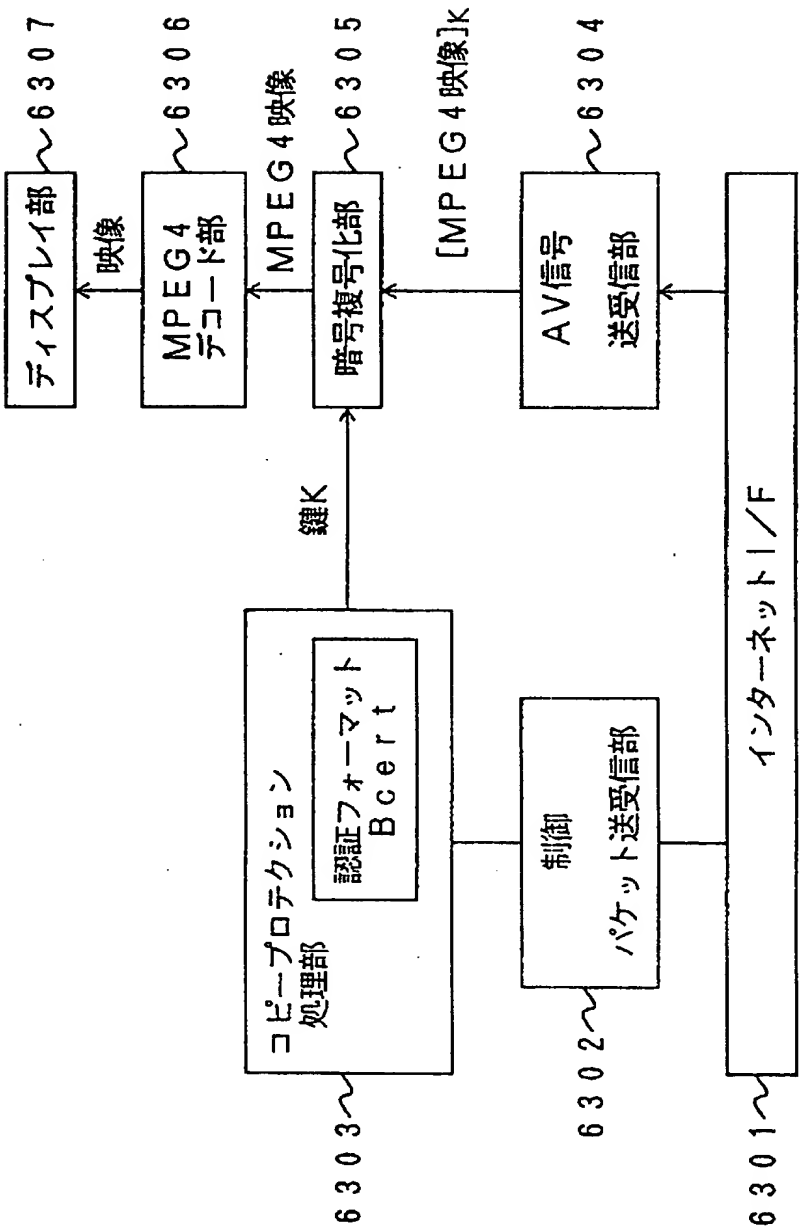
【図５９】


MPEG
ストレージ部
6406
MPEG映像
暗号化部
6405
[MPEG映像]K
ISO信号
送受信部
6404
鍵K
コピープロテクション
処理部
認証フォーマット
Acert
6403
AV／Cプロトコル
処理部
6402
IEEE1394 I／F
6401

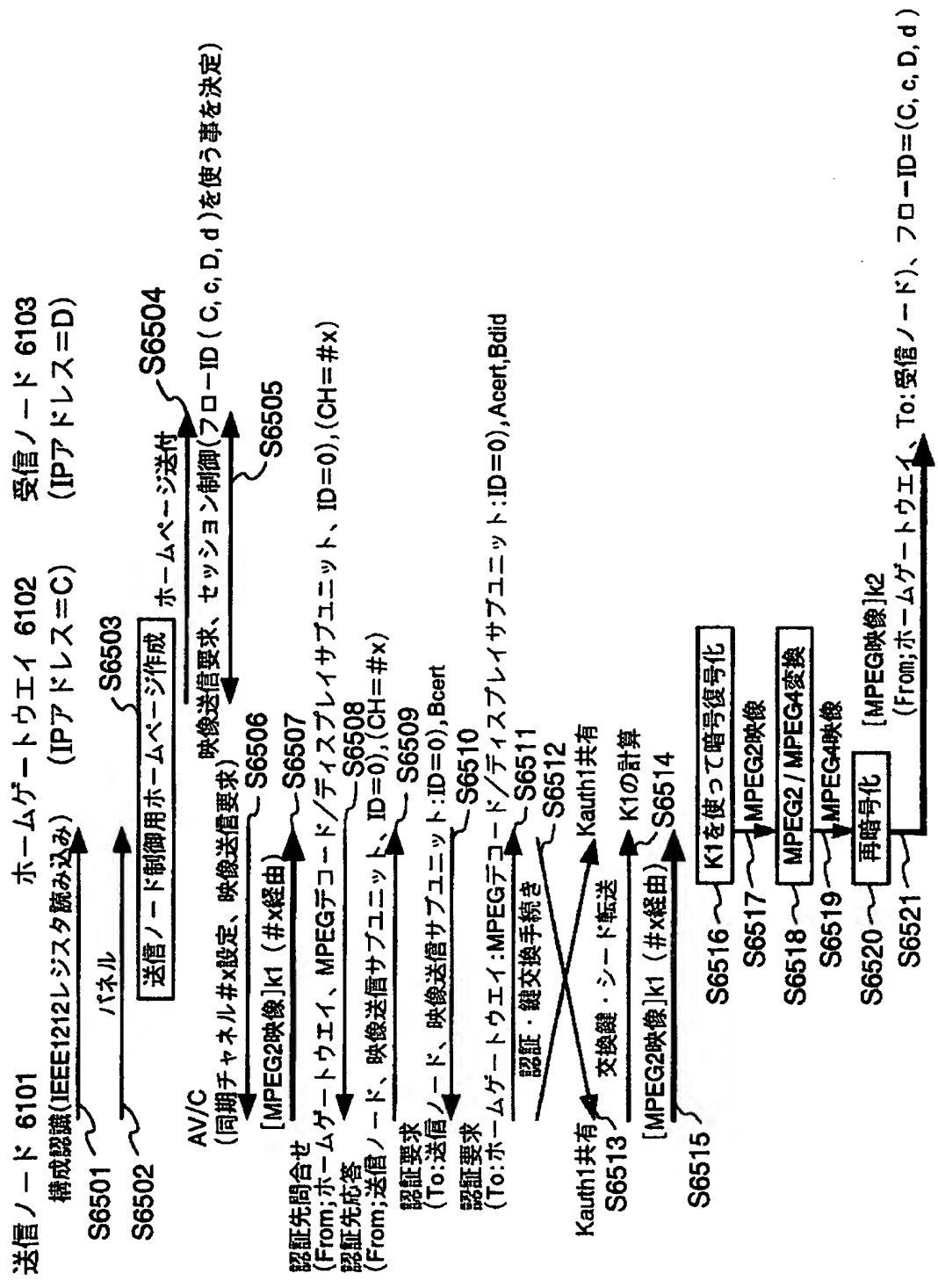
【図６０】


6211
ホームページ
作成・蓄積部
6212
インターネット側
プロテクション処理部
認証フォーマット
Ccert
制御パケット
送受信部
6213
インターネットI／F
6202
インターネット
6215
6214
MPEG4映像
鍵K2
[MPEG
[4映像
]K2
AV信号
送受信部
6206
6210
代理ホームページ作成部
変換テーブル
MPEG2／MPEG4
変換部
暗号化部
6205
MPEG2映像
6204
暗号
複号化部
鍵K1
[MPEG
[2映像
]K1
ISO信号
送受信部
6203
6208
IEEE1394コピー
プロテクション処理部
認証フォーマット
Bcert
AV／Cプロトコル
処理部
6207
IEEE1394 I／F
6201
IEEE1394バス
6209
1394バス
構成認識部

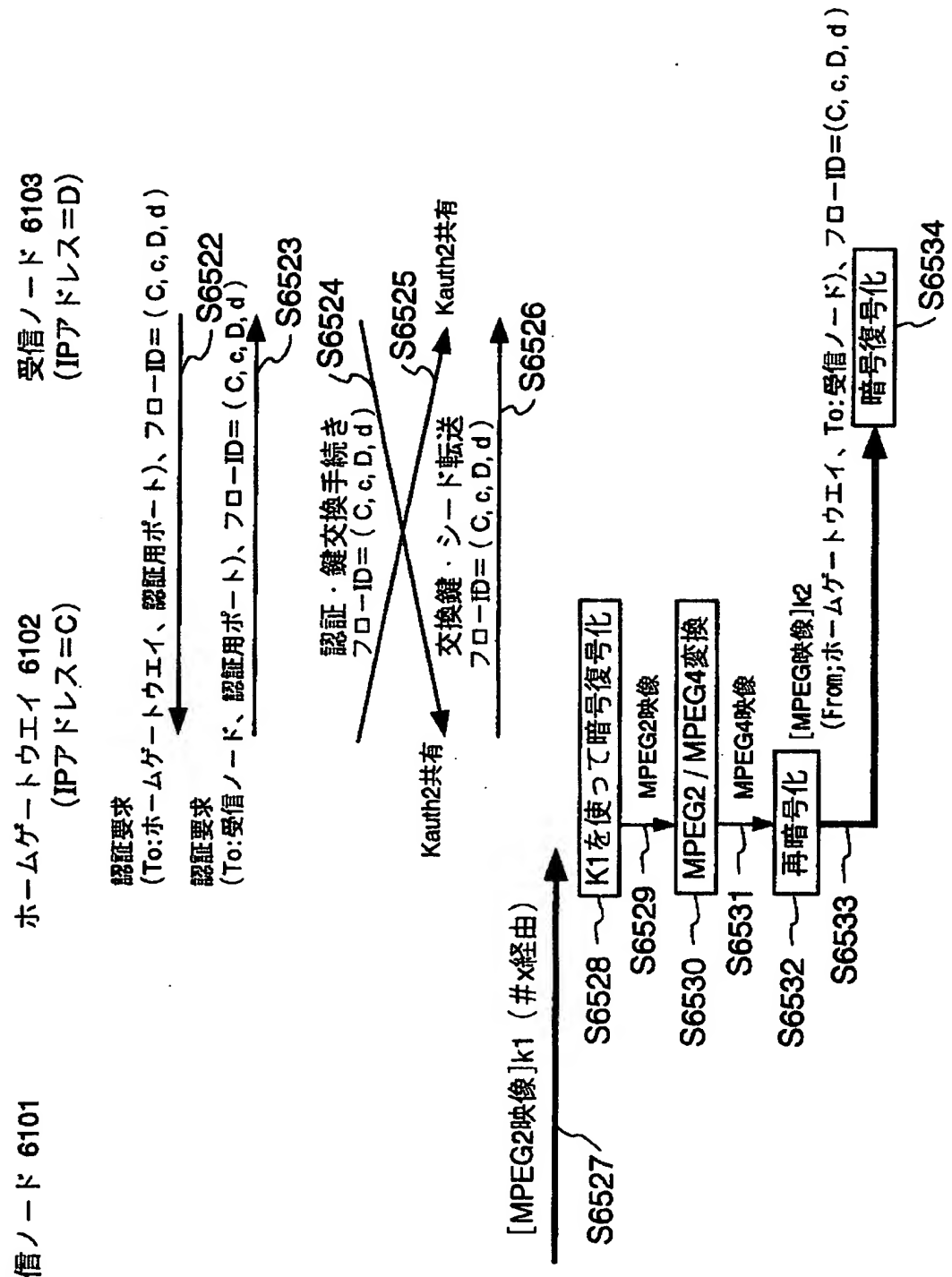
【図６１】


ディスプレイ部
6307
映像
MPEG4
デコード部
6306
MPEG4映像
暗号複号化部
6305
[MPEG4映像]k
AV信号
送受信部
6304
鍵K
コピープロテクション
処理部
認証フォーマット
Bcert
6303
制御
パケット送受信部
6302
インターネットI／F
6301

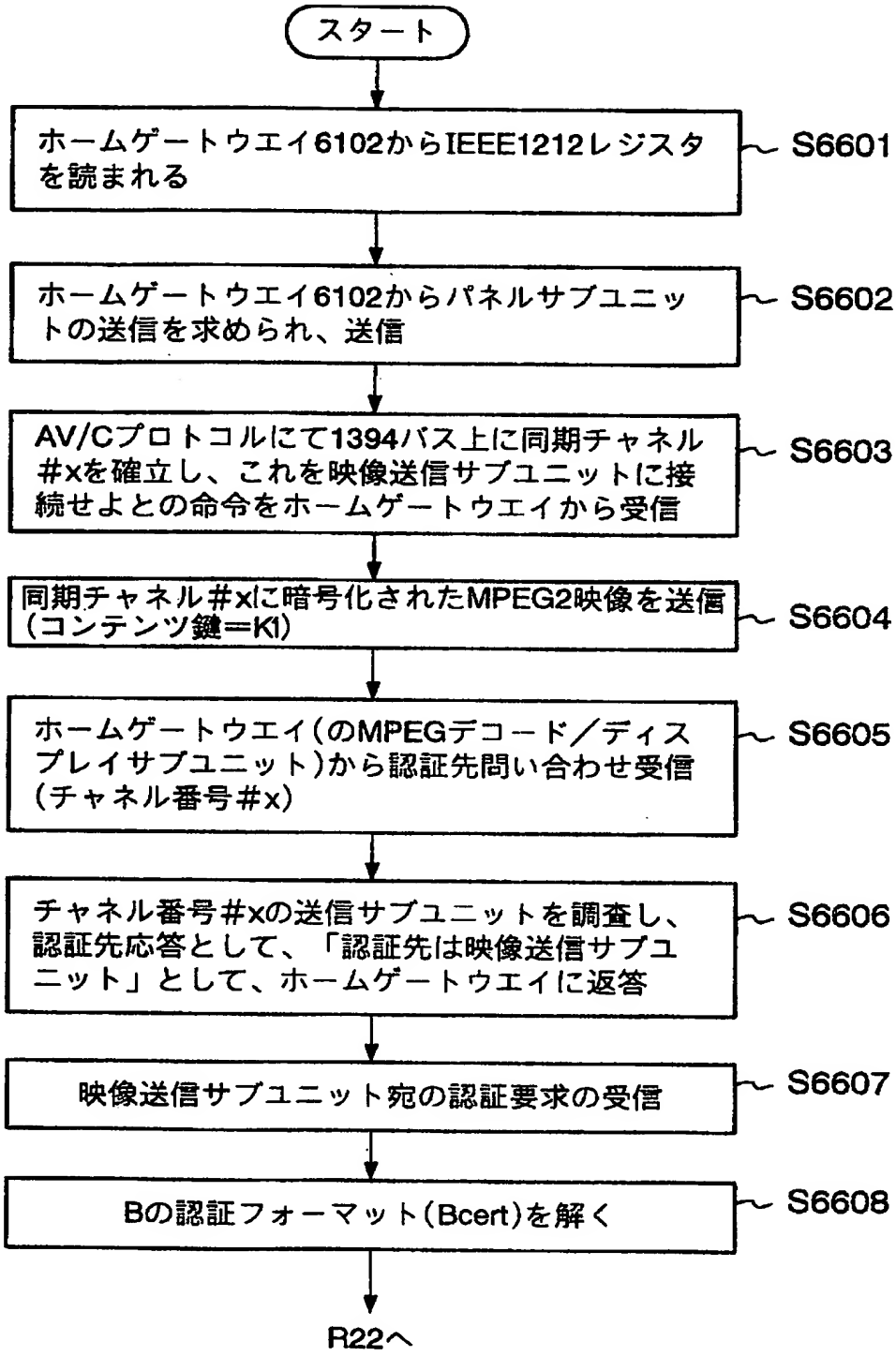
【図６２】


送信ノード 6101
ホームゲートウエイ 6102
受信ノード 6103
(IPアドレス=C)
(IPアドレス=D)
構成認識(IEEE1212レジスタ読み込み)
S6501
パネル
S6502
S6503
送信ノード制御用ホームページ作成
ホームページ送付
S6504
AV/C
(同期チャネル#x設定、映像送信要求)
映像送信要求、セッション制御(フローID(C, c, D, d)を使う事を決定)
S6505
[MPEG2映像]k1 (#x経由)
S6506
認証先問合せ
(From;ホームゲートウエイ、MPEGデコード/ディスプレイサブユニット、ID=0),(CH=#x)
S6507
認証先応答
(From;送信ノード、映像送信サブユニット、ID=0),(CH=#x)
S6508
認証要求
(To:送信ノード、映像送信サブユニット:ID=0),Bcert
S6509
S6510
認証要求
(To:ホームゲートウエイ:MPEGデコード/ディスプレイサブユニット:ID=0),Acert,Bdid
S6511
認証・鍵交換手続き
S6512
Kauth1共有
S6513
交換鍵・シード転送
Kauth1共有
K1の計算
S6514
[MPEG2映像]k1 (#x経由)
S6515
K1を使って暗号復号化
S6516
MPEG2映像
S6517
MPEG2/MPEG4変換
S6518
MPEG4映像
S6519
再暗号化
S6520
[MPEG映像]k2
(From;ホームゲートウエイ、To:受信ノード)、フローID=(C, c, D, d)
S6521

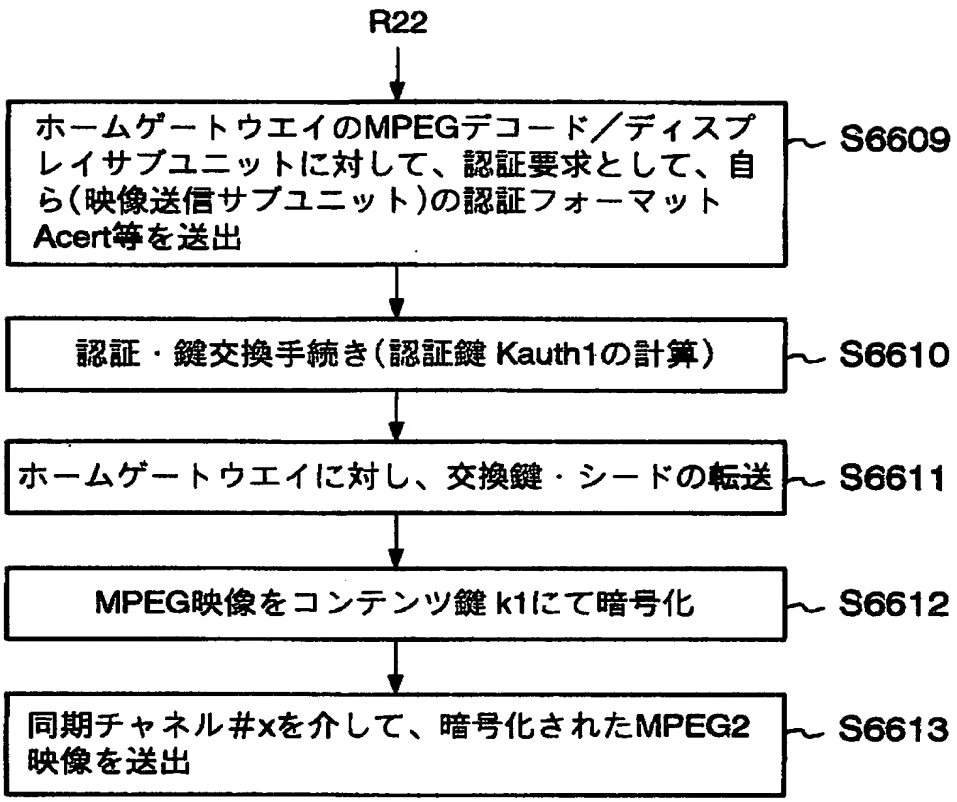
【図６３】


送信ノード 6101
ホームゲートウエイ 6102
(IPアドレス=C)
受信ノード 6103
(IPアドレス=D)
認証要求
(To:ホームゲートウエイ、認証用ポート)、フローID=(C, c, D, d)
S6522
認証要求
(To:受信ノード、認証用ポート)、フローID=(C, c, D, d)
S6523
S6524
認証・鍵交換手続き
フローID=(C, c, D, d)
S6525
Kauth2共有
交換鍵・シード転送
フローID=(C, c, D, d)
S6526
Kauth2共有
[MPEG2映像]k1 (#x経由)
S6527
S6528
K1を使って暗号復号化
S6529
MPEG2映像
S6530
MPEG2 / MPEG4変換
S6531
MPEG4映像
S6532
再暗号化
S6533
[MPEG映像]k2
(From;ホームゲートウエイ、To:受信ノード)、フローID=(C, c, D, d)
暗号復号化
S6534

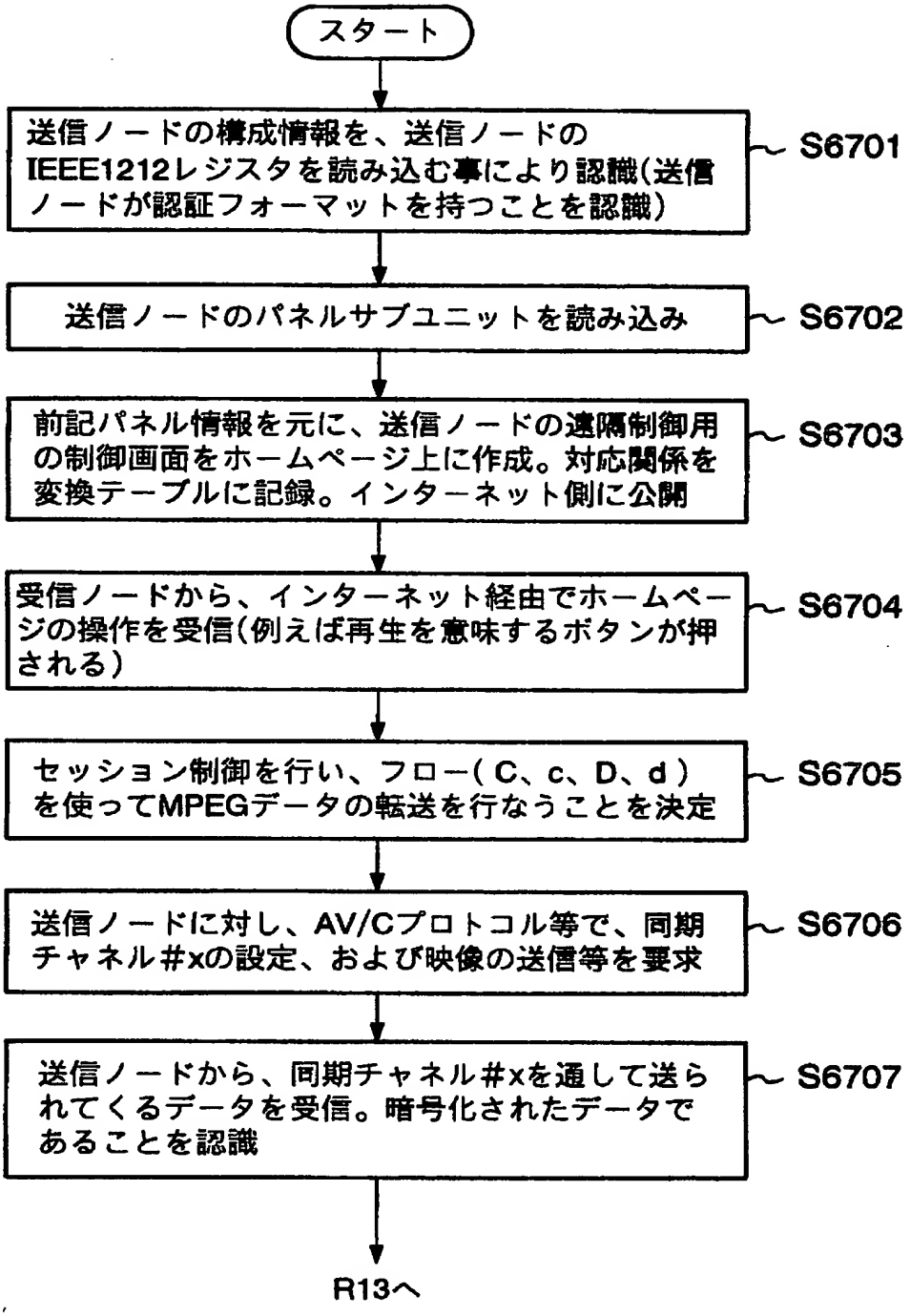
【図６４】


スタート
ホームゲートウエイ6102からIEEE1212レジスタを読まれる
S6601
ホームゲートウエイ6102からパネルサブユニットの送信を求められ、送信
S6602
AV/Cプロトコルにて1394バス上に同期チャネル#xを確立し、これを映像送信サブユニットに接続せよとの命令をホームゲートウエイから受信
S6603
同期チャネル#xに暗号化されたMPEG2映像を送信(コンテンツ鍵＝K1)
S6604
ホームゲートウエイ(のMPEGデコード／ディスプレイサブユニット)から認証先問い合わせ受信(チャネル番号#x)
S6605
チャネル番号#xの送信サブユニットを調査し、認証先応答として、「認証先は映像送信サブユニット」として、ホームゲートウエイに返答
S6606
映像送信サブユニット宛の認証要求の受信
S6607
Bの認証フォーマット(Bcert)を解く
S6608
R22へ

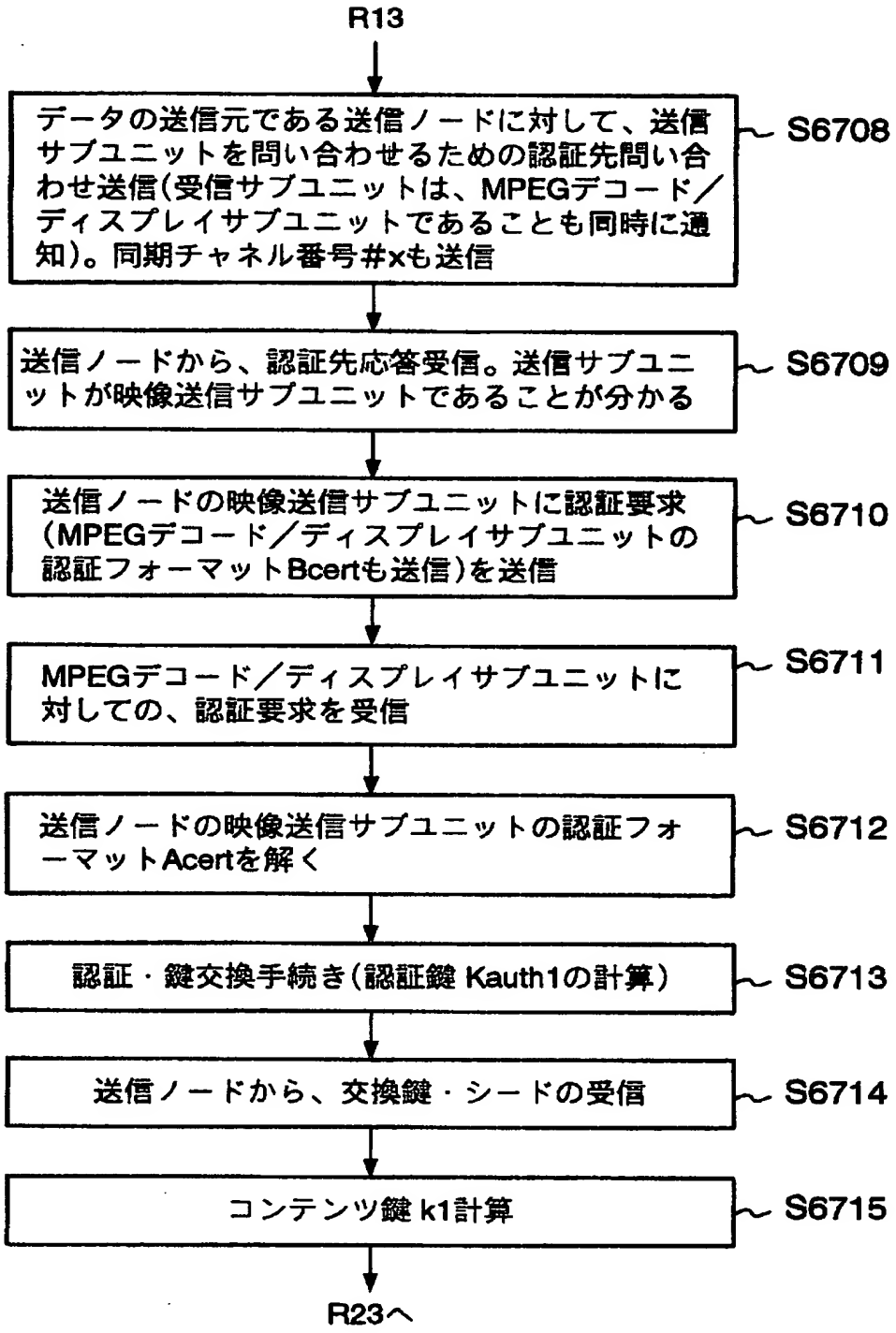
【図６５】


R22
ホームゲートウエイのMPEGデコード／ディスプレイサブユニットに対して、認証要求として、自ら(映像送信サブユニット)の認証フォーマットAcert等を送出
S6609
認証・鍵交換手続き(認証鍵 Kauth1の計算)
S6610
ホームゲートウエイに対し、交換鍵・シードの転送
S6611
MPEG映像をコンテンツ鍵 k1にて暗号化
S6612
同期チャネル#xを介して、暗号化されたMPEG2映像を送出
S6613

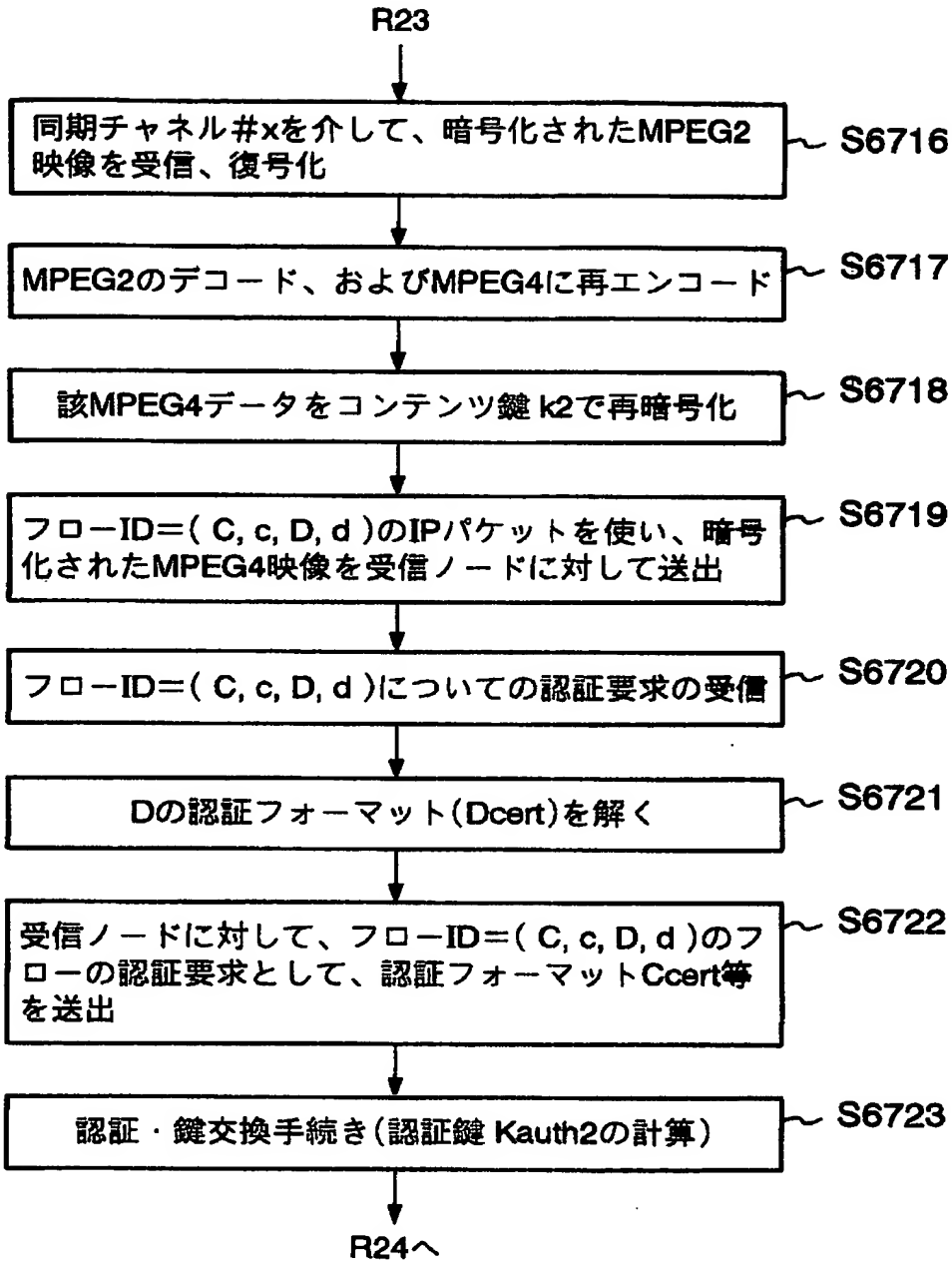
【図６６】


スタート
送信ノードの構成情報を、送信ノードのIEEE1212レジスタを読み込む事により認識(送信ノードが認証フォーマットを持つことを認識)
S6701
送信ノードのパネルサブユニットを読み込み
S6702
前記パネル情報を元に、送信ノードの遠隔制御用の制御画面をホームページ上に作成。対応関係を変換テーブルに記録。インターネット側に公開
S6703
受信ノードから、インターネット経由でホームページの操作を受信(例えば再生を意味するボタンが押される)
S6704
セッション制御を行い、フロー(C、c、D、d)を使ってMPEGデータの転送を行なうことを決定
S6705
送信ノードに対し、AV/Cプロトコル等で、同期チャネル#xの設定、および映像の送信等を要求
S6706
送信ノードから、同期チャネル#xを通して送られてくるデータを受信。暗号化されたデータであることを認識
S6707
R13へ

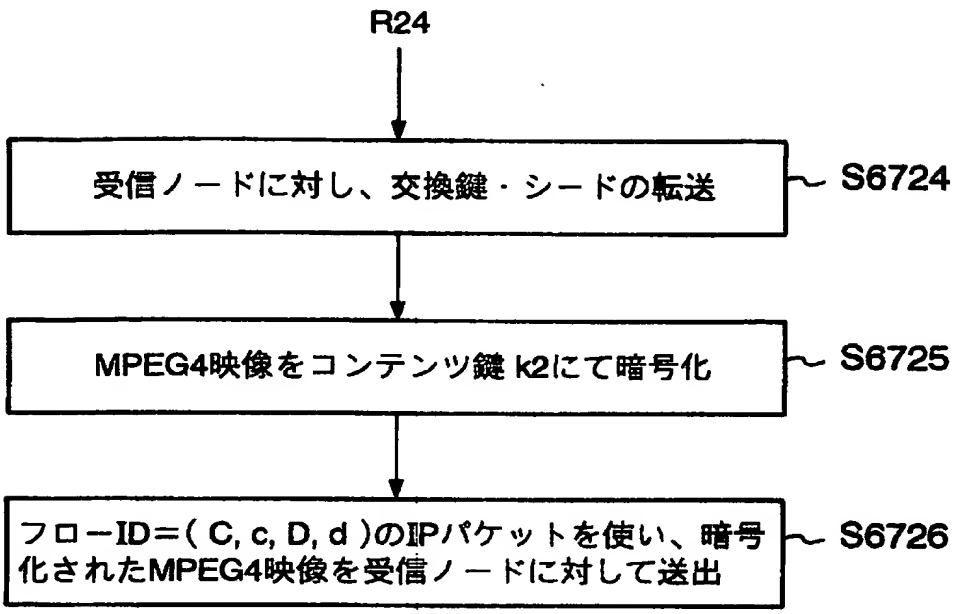
【図６７】


R13
データの送信元である送信ノードに対して、送信サブユニットを問い合わせるための認証先問い合わせ送信(受信サブユニットは、MPEGデコード／ディスプレイサブユニットであることも同時に通知)。同期チャネル番号#xも送信
S6708
送信ノードから、認証先応答受信。送信サブユニットが映像送信サブユニットであることが分かる
S6709
送信ノードの映像送信サブユニットに認証要求(MPEGデコード／ディスプレイサブユニットの認証フォーマットBcertも送信)を送信
S6710
MPEGデコード／ディスプレイサブユニットに対しての、認証要求を受信
S6711
送信ノードの映像送信サブユニットの認証フォーマットAcertを解く
S6712
認証・鍵交換手続き(認証鍵 Kauth1の計算)
S6713
送信ノードから、交換鍵・シードの受信
S6714
コンテンツ鍵 k1計算
S6715
R23へ

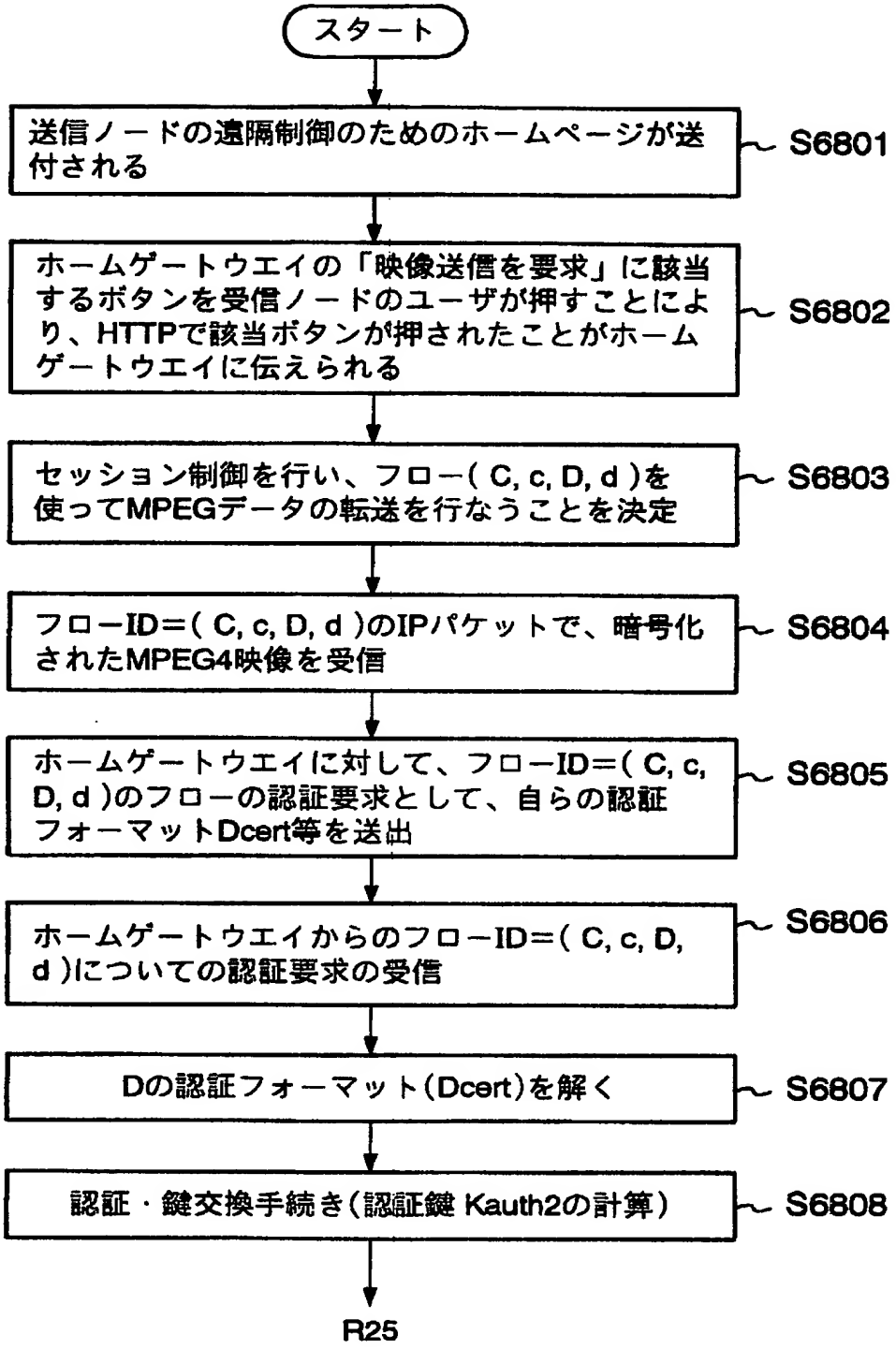
【図６８】


R23
同期チャネル#xを介して、暗号化されたMPEG2映像を受信、復号化
S6716
MPEG2のデコード、およびMPEG4に再エンコード
S6717
該MPEG4データをコンテンツ鍵k2で再暗号化
S6718
フローID=(C, c, D, d)のIPパケットを使い、暗号化されたMPEG4映像を受信ノードに対して送出
S6719
フローID=(C, c, D, d)についての認証要求の受信
S6720
Dの認証フォーマット(Dcert)を解く
S6721
受信ノードに対して、フローID=(C, c, D, d)のフローの認証要求として、認証フォーマットCcert等を送出
S6722
認証・鍵交換手続き(認証鍵 Kauth2の計算)
S6723
R24へ

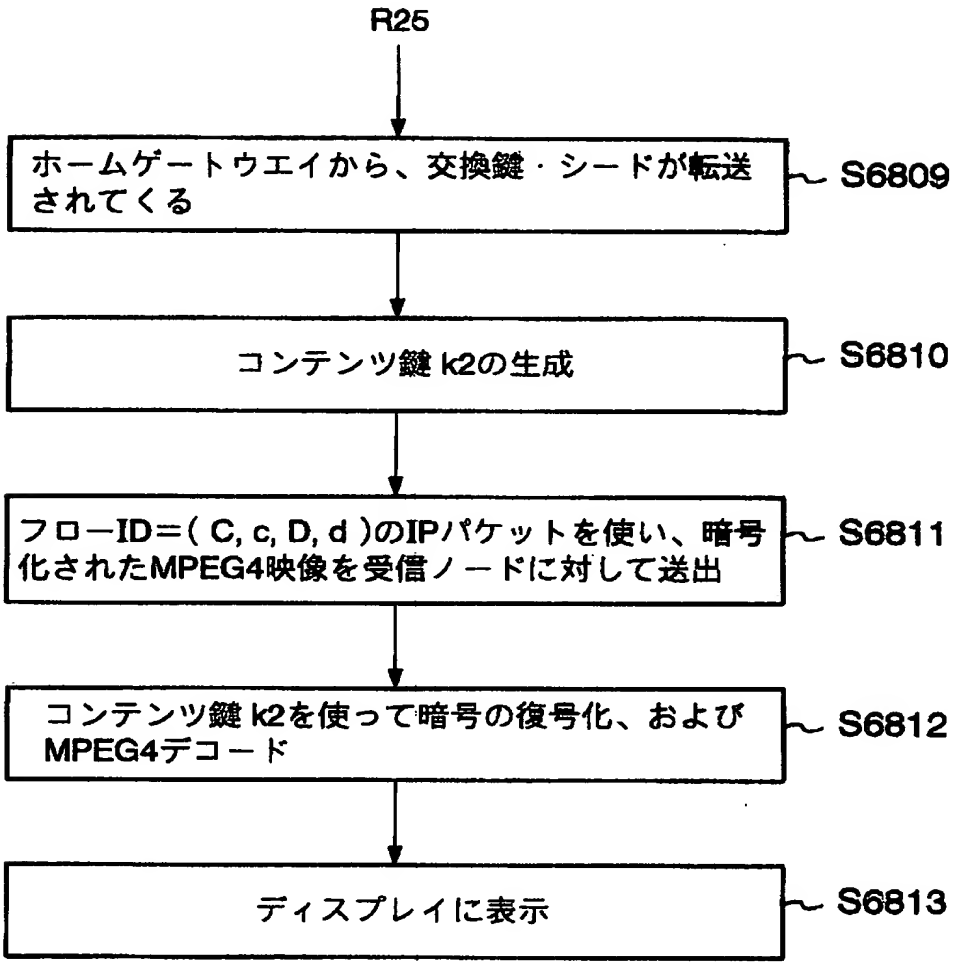
【図６９】


R24
受信ノードに対し、交換鍵・シードの転送
S6724
MPEG4映像をコンテンツ鍵 k2にて暗号化
S6725
フローID＝(C, c, D, d)のIPパケットを使い、暗号化されたMPEG4映像を受信ノードに対して送出
S6726

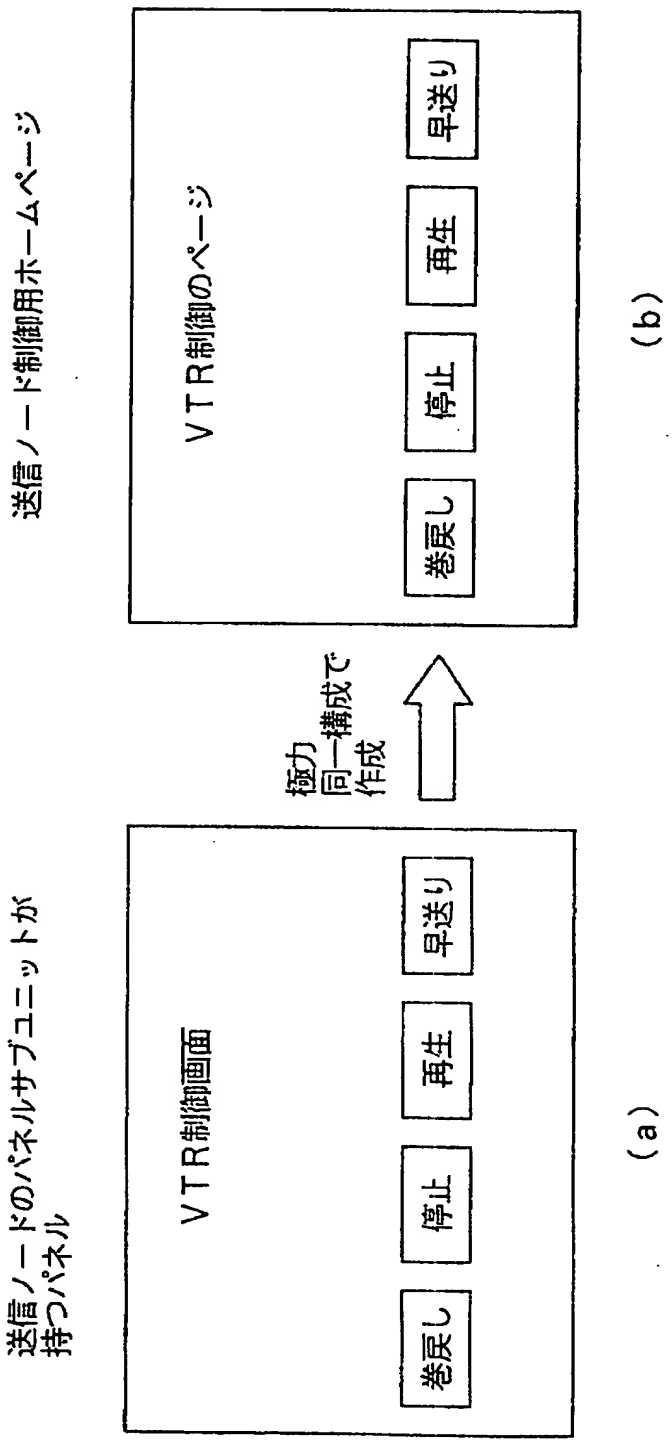
【図７０】


スタート
送信ノードの遠隔制御のためのホームページが送付される
S6801
ホームゲートウエイの「映像送信を要求」に該当するボタンを受信ノードのユーザが押すことにより、HTTPで該当ボタンが押されたことがホームゲートウエイに伝えられる
S6802
セッション制御を行い、フロー(C, c, D, d)を使ってMPEGデータの転送を行なうことを決定
S6803
フローID=(C, c, D, d)のIPパケットで、暗号化されたMPEG4映像を受信
S6804
ホームゲートウエイに対して、フローID=(C, c, D, d)のフローの認証要求として、自らの認証フォーマットDcert等を送出
S6805
ホームゲートウエイからのフローID=(C, c, D, d)についての認証要求の受信
S6806
Dの認証フォーマット(Dcert)を解く
S6807
認証・鍵交換手続き(認証鍵 Kauth2の計算)
S6808
R25

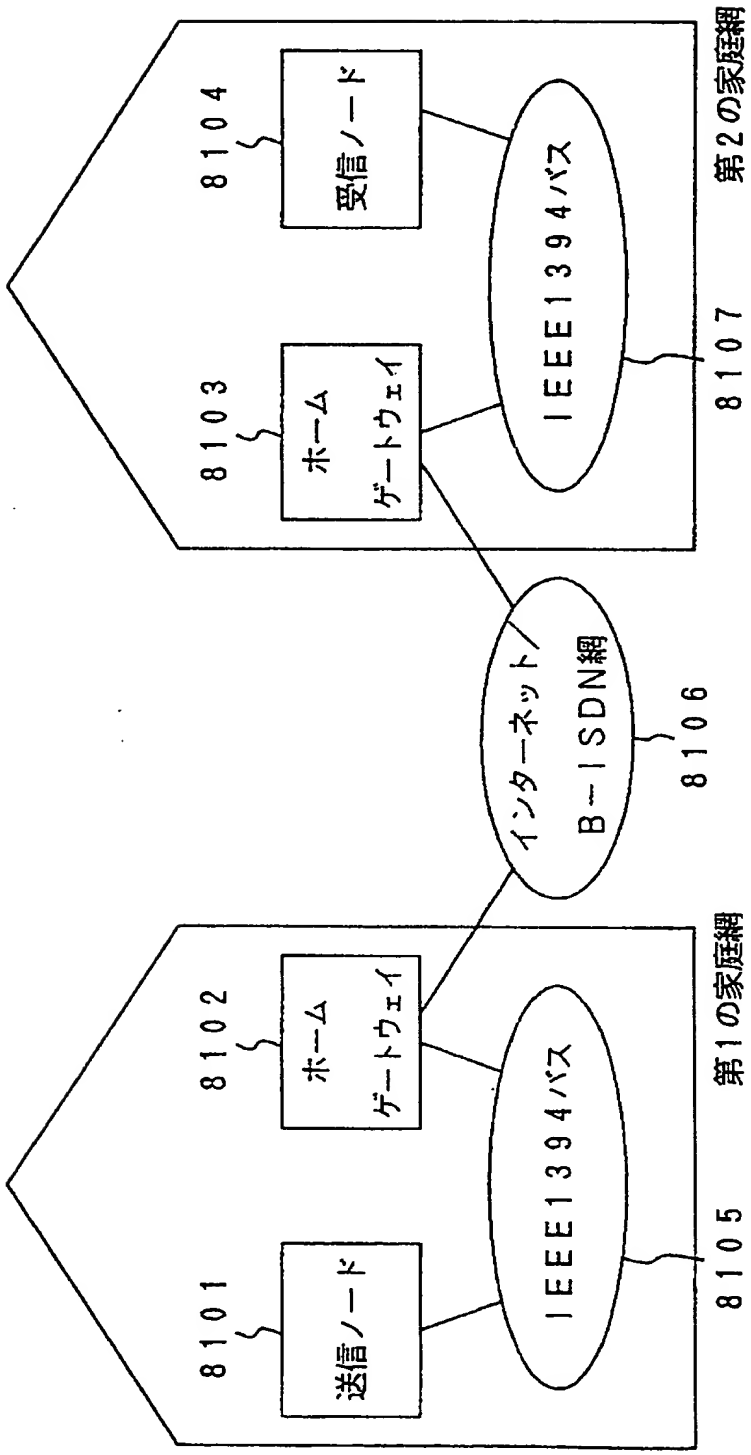
【図７１】


R25
ホームゲートウエイから、交換鍵・シードが転送されてくる
S6809
コンテンツ鍵k2の生成
S6810
フローID＝(C, c, D, d)のIPパケットを使い、暗号化されたMPEG4映像を受信ノードに対して送出
S6811
コンテンツ鍵k2を使って暗号の復号化、およびMPEG4デコード
S6812
ディスプレイに表示
S6813

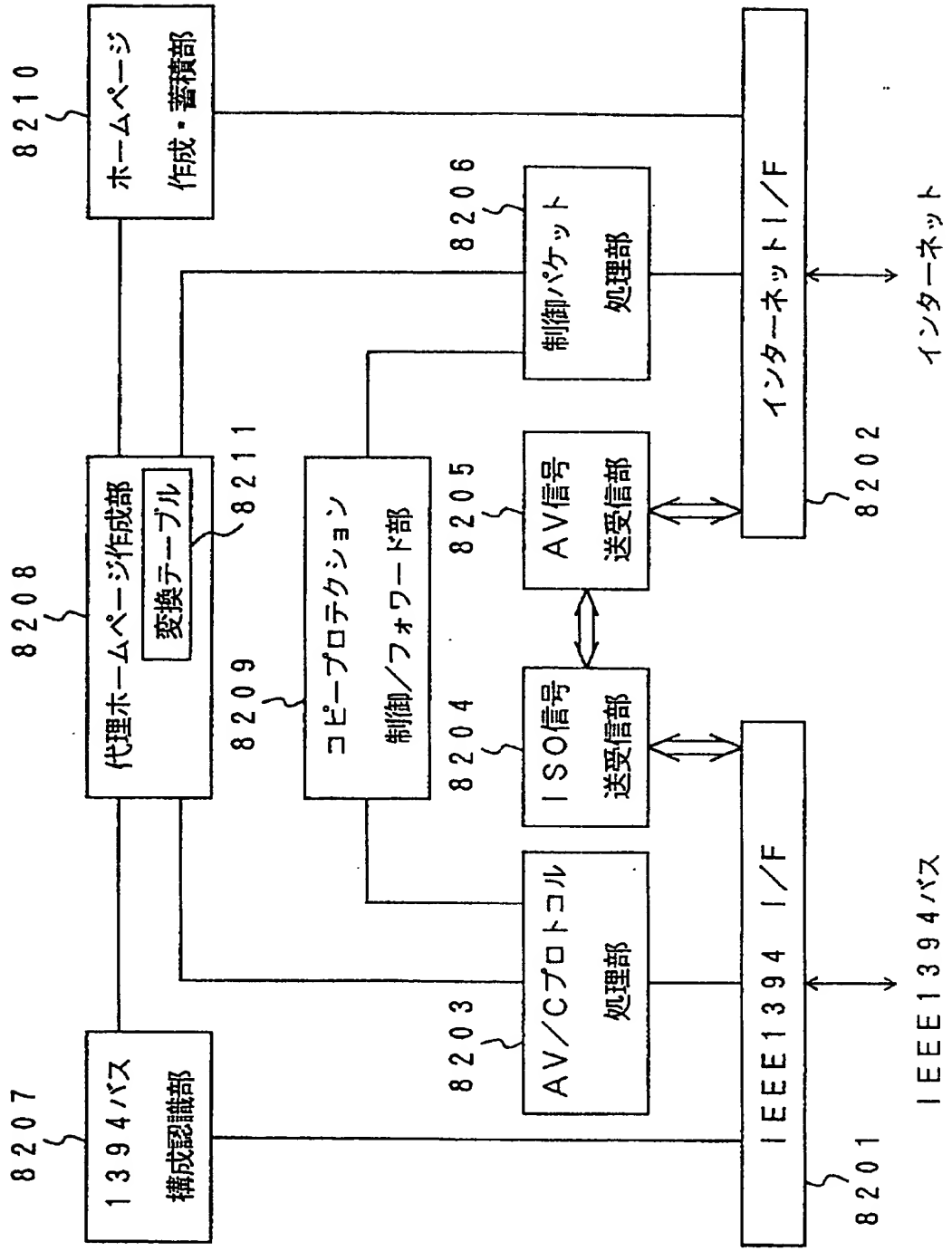
【図７２】


送信ノード制御用ホームページ
VTR制御のページ
巻戻し
停止
再生
早送り
極力
同一構成で
作成
(b)
送信ノードのパネルサブユニットが
持つパネル
VTR制御画面
巻戻し
停止
再生
早送り
(a)

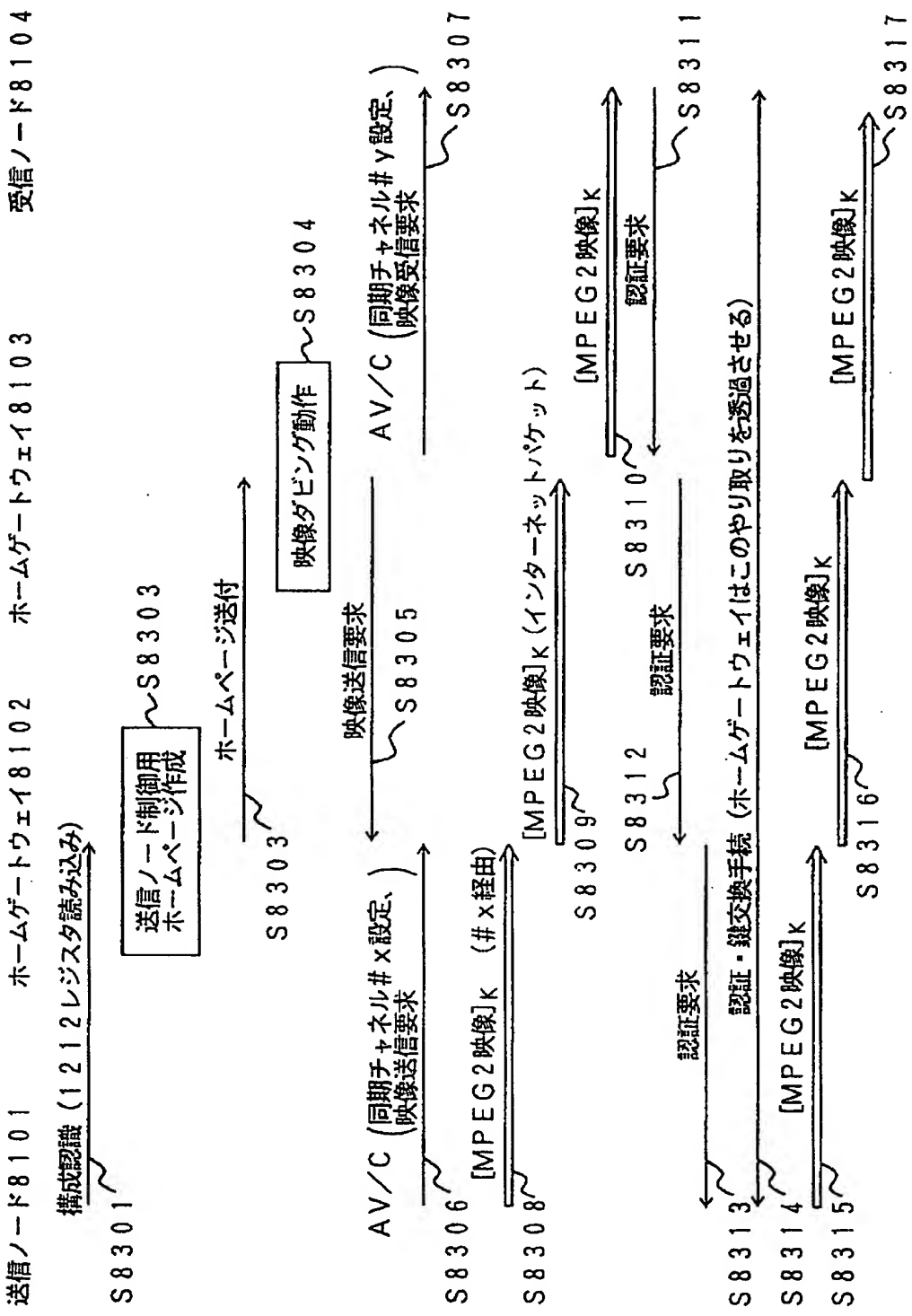
【図７３】


8101
送信ノード
8102
ホーム
ゲートウェイ
IEEE1394バス
8105
第1の家庭網
インターネット
B－ISDN網
8106
8103
ホーム
ゲートウェイ
8104
受信ノード
IEEE1394バス
8107
第2の家庭網

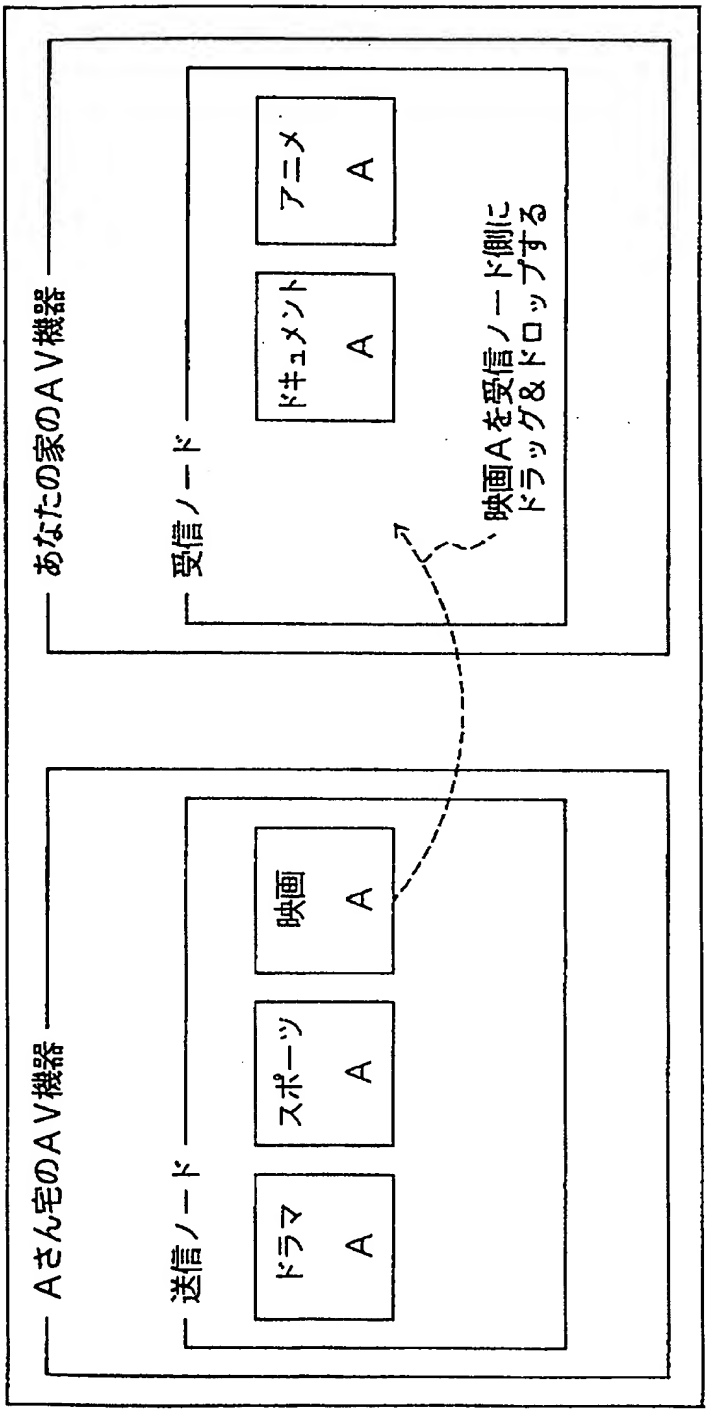
【図７４】


８２１０
ホームページ
作成・蓄積部
８２０６
制御パケット
処理部
インターネットI／F
インターネット
８２０８
代理ホームページ作成部
変換テーブル
８２１１
８２０９
コピープロテクション
制御／フォワード部
８２０５
AV信号
送受信部
８２０２
８２０４
ISO信号
送受信部
８２０７
１３９４バス
構成認識部
８２０３
AV／Cプロトコル
処理部
IEEE１３９４ I／F
８２０１
IEEE１３９４バス

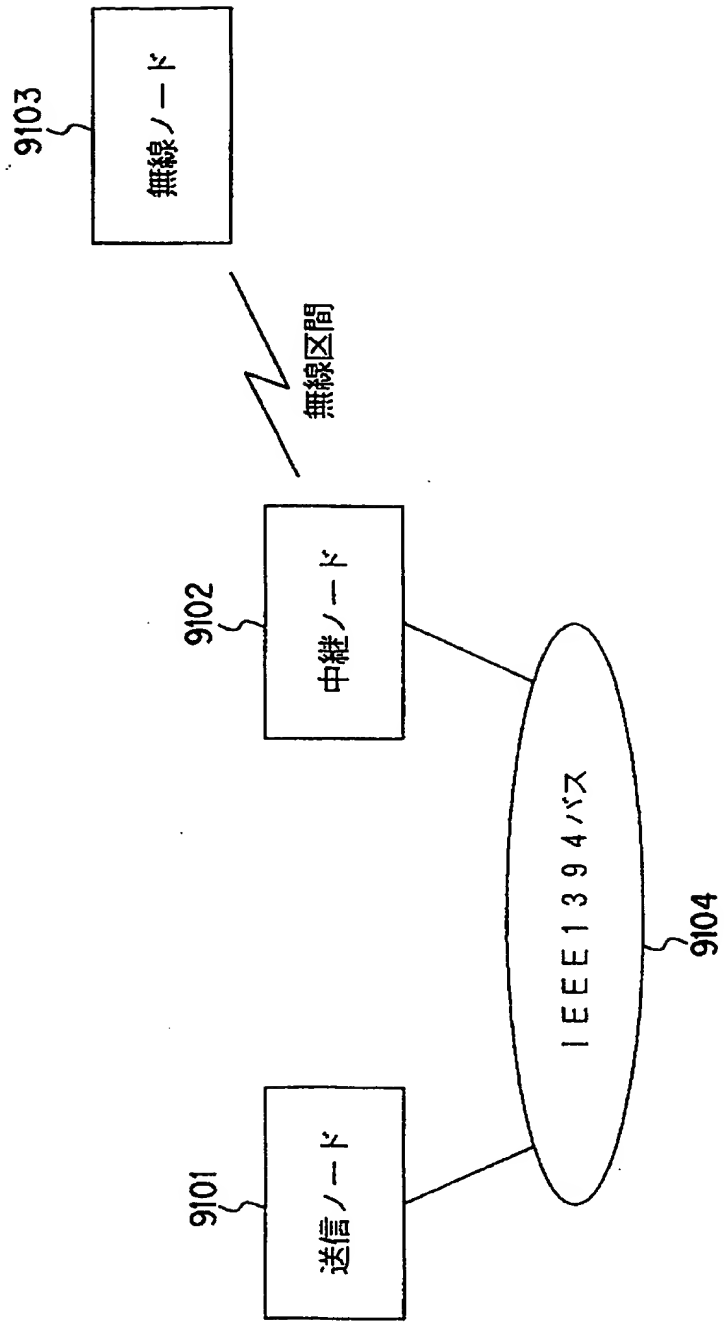
【図７５】


送信ノード８１０１
ホームゲートウェイ８１０２
ホームゲートウェイ８１０３
受信ノード８１０４
構成認識（１２１２レジスタ読み込み）
S８３０１
送信ノード制御用ホームページ作成
S８３０３
S８３０２
ホームページ送付
S８３０４
映像ダビング動作
AV／C（同期チャネル#y設定、映像受信要求）
S８３０７
映像送信要求
S８３０５
AV／C（同期チャネル#x設定、映像送信要求）
S８３０６
[MPEG2映像]K（#x経由）
S８３０８
[MPEG2映像]K（インターネットパケット）
S８３０９
[MPEG2映像]K
S８３１０
認証要求
S８３１１
S８３１２
認証要求
認証要求
S８３１３
認証・鍵交換手続（ホームゲートウェイはこのやり取りを透過させる）
S８３１４
[MPEG2映像]K
S８３１５
[MPEG2映像]K
S８３１６
[MPEG2映像]K
S８３１７

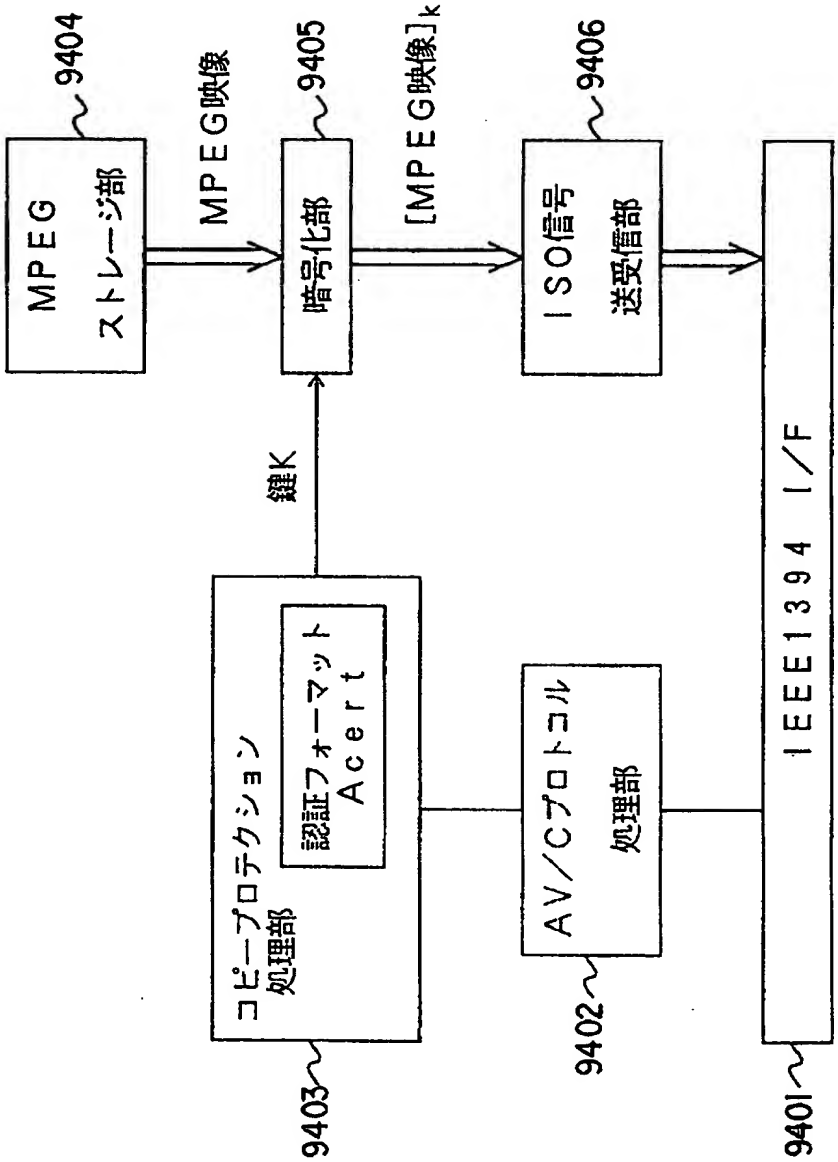
【図７６】


Aさん宅のAV機器
送信ノード
ドラマ A
スポーツ A
映画 A
あなたの家のAV機器
受信ノード
ドキュメント A
アニメ A
映画Aを受信ノード側に
ドラッグ&ドロップする

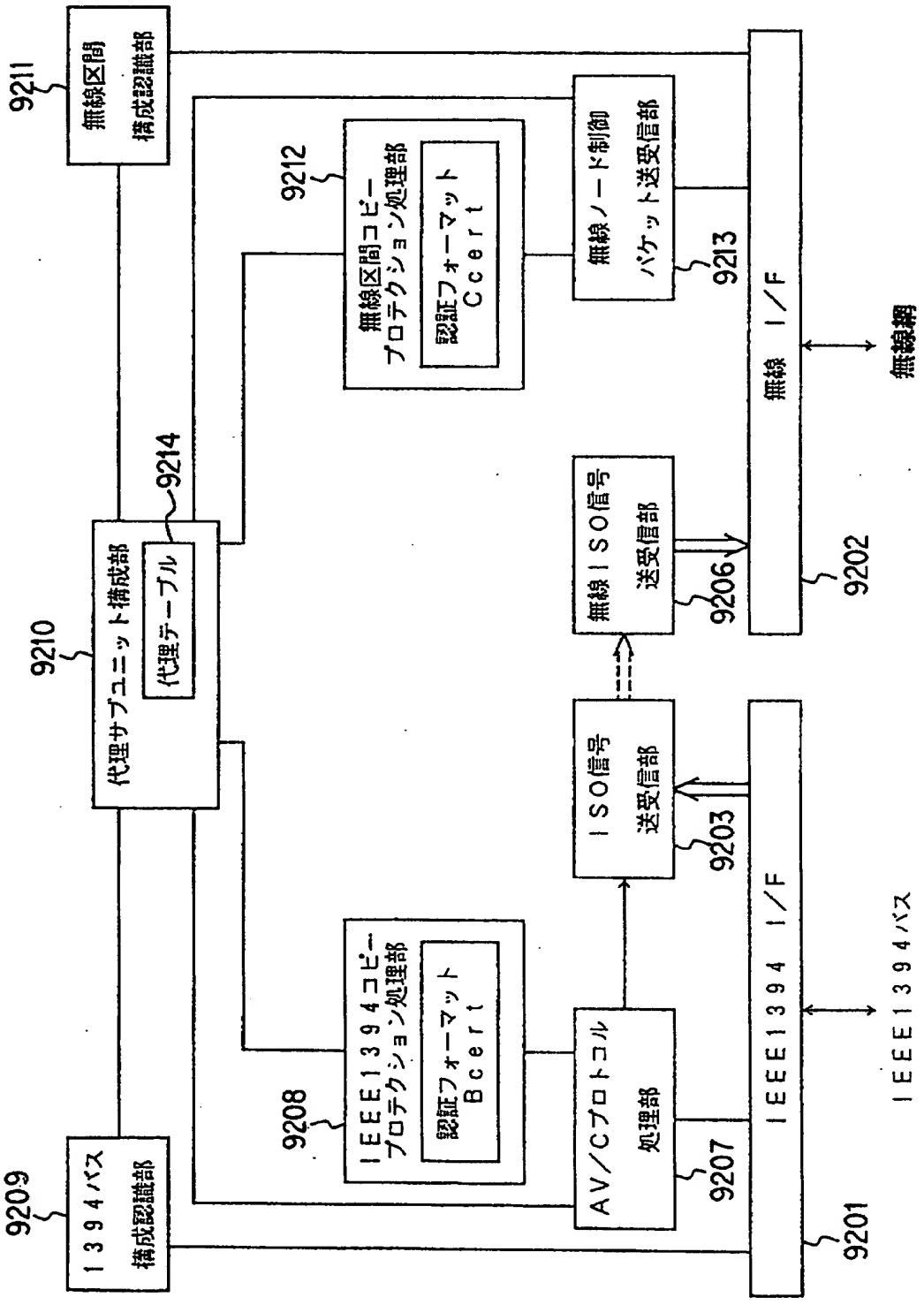
【図７７】



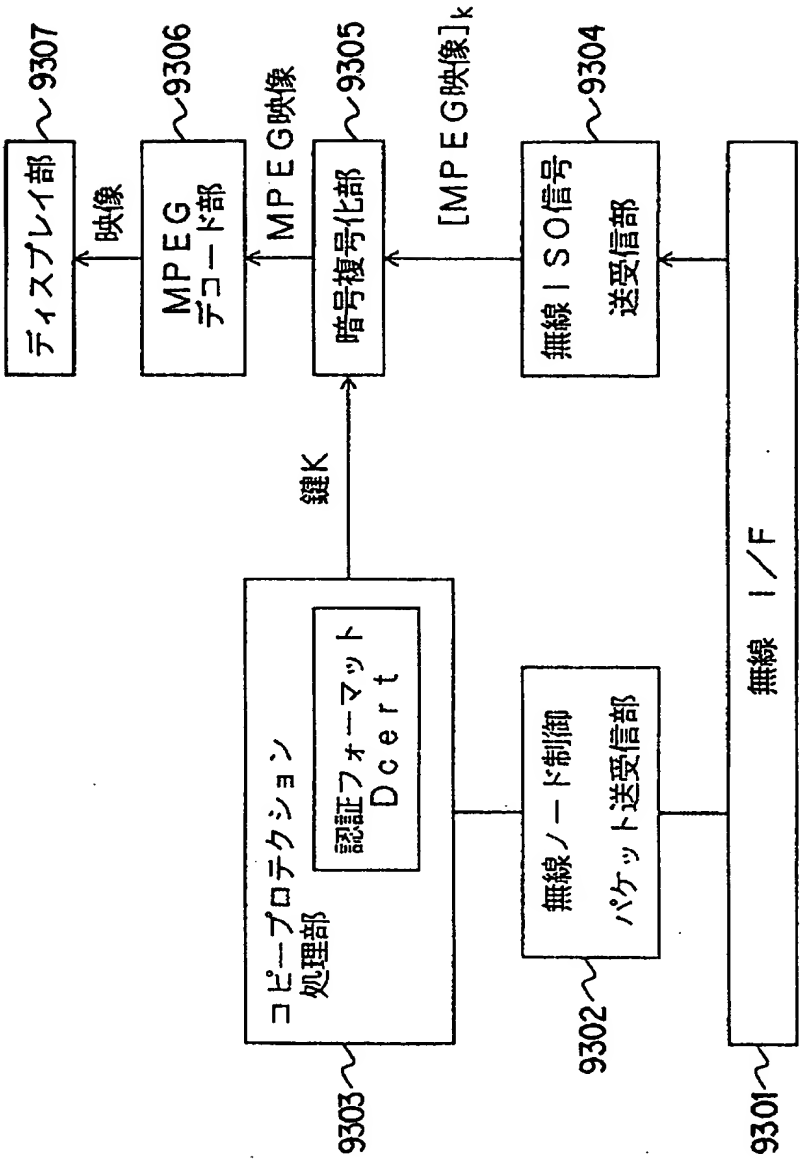
【図７８】


MPEG
ストレージ部
9404
MPEG映像
暗号化部
9405
[MPEG映像]k
ISO信号
送受信部
9406
鍵K
コピープロテクション
処理部
認証フォーマット
Acert
9403
AV/Cプロトコル
処理部
9402
IEEE1394 I/F
9401

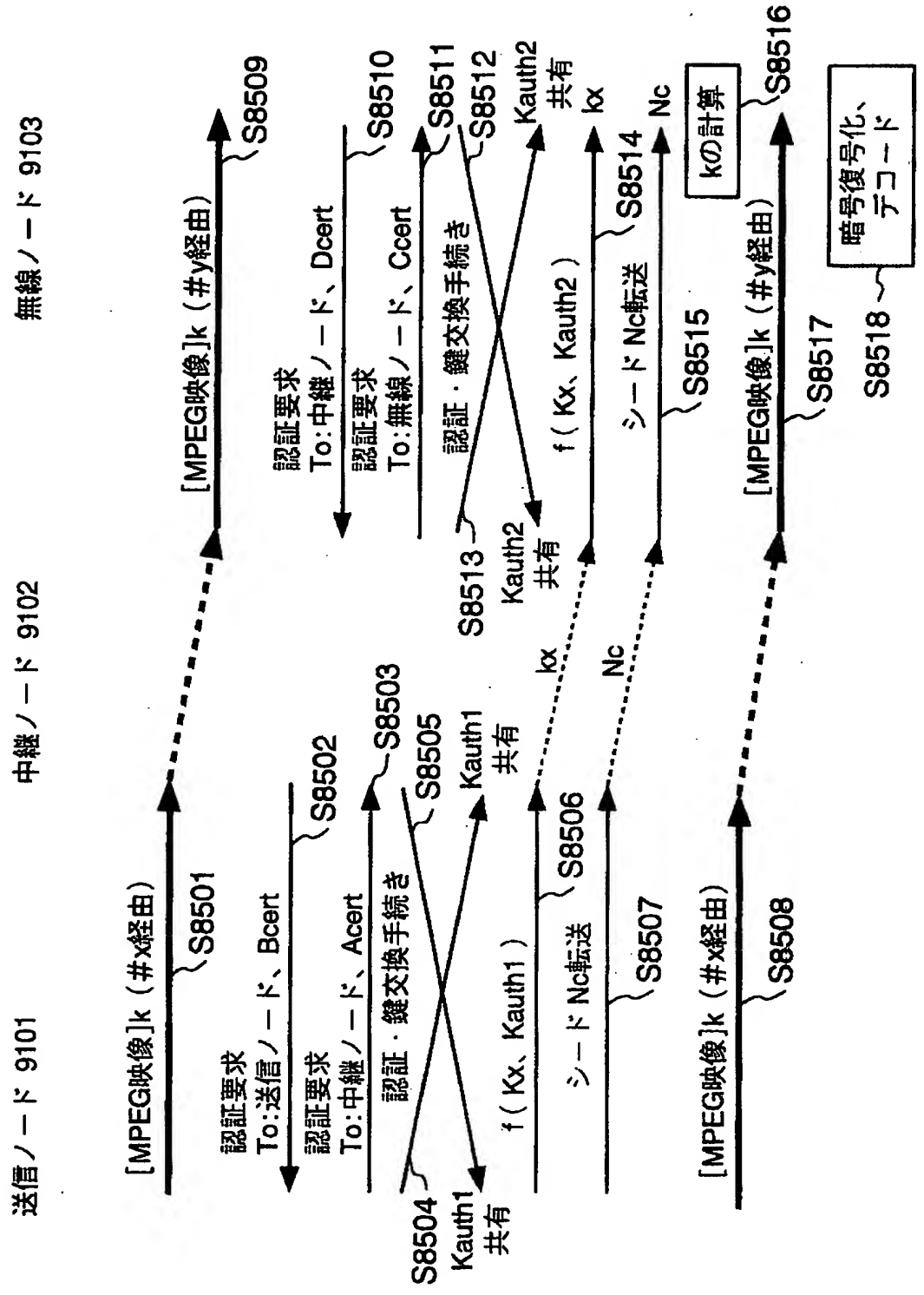
【図７９】


9211
無線区間
構成認識部
9212
無線区間コピー
プロテクション処理部
認証フォーマット
Ccert
無線ノード制御
パケット送受信部
9213
9214
代理サブユニット構成部
代理テーブル
9210
無線ＩＳＯ信号
送受信部
9206
無線　Ｉ／Ｆ
9202
無線網
ＩＳＯ信号
送受信部
9203
9209
１３９４バス
構成認識部
9208
ＩＥＥＥ１３９４コピー
プロテクション処理部
認証フォーマット
Bcert
ＡＶ／Ｃプロトコル
処理部
9207
ＩＥＥＥ１３９４　Ｉ／Ｆ
9201
ＩＥＥＥ１３９４バス

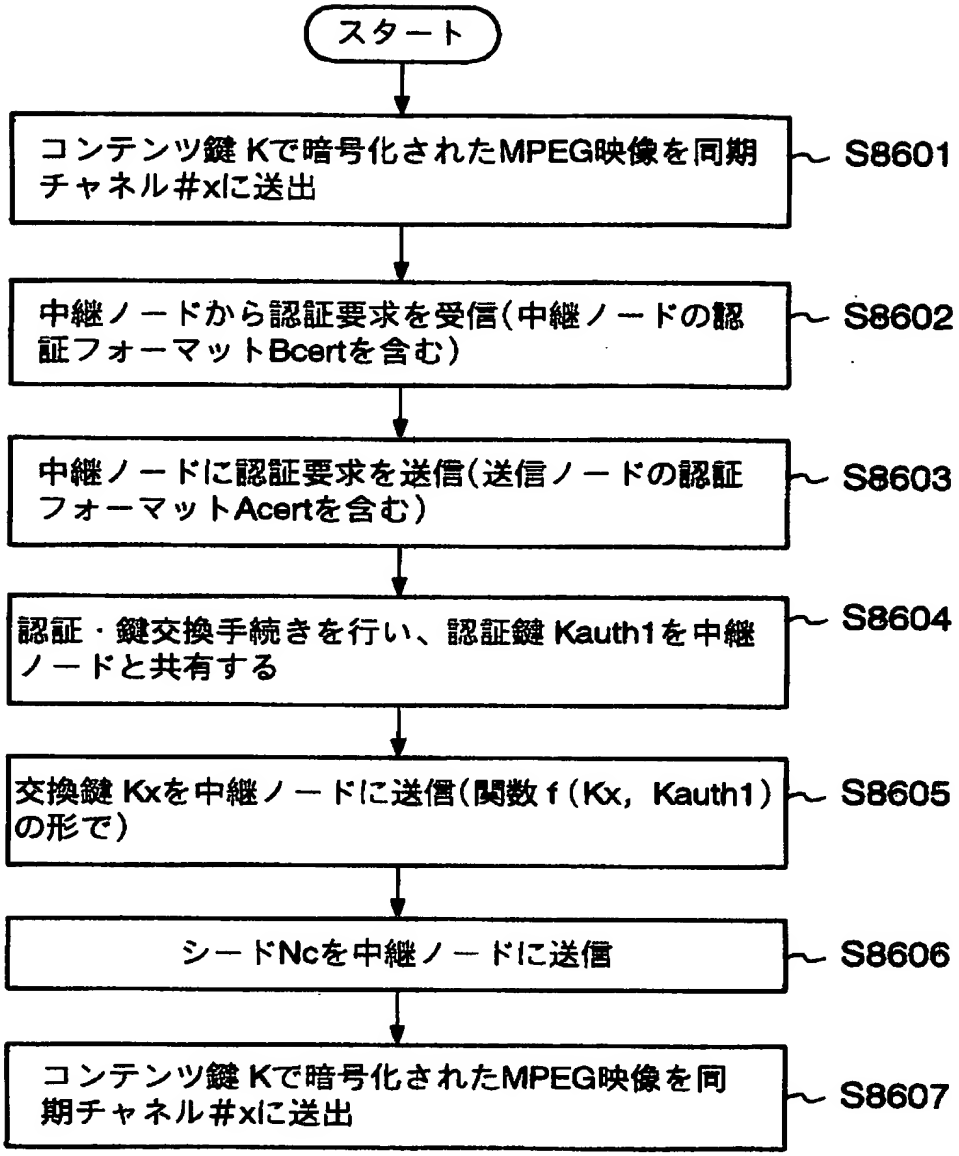
【図８０】


ディスプレイ部
9307
映像
MPEG
デコード部
9306
MPEG映像
暗号複号化部
9305
[MPEG映像]k
無線ISO信号
送受信部
9304
鍵K
コピープロテクション
処理部
認証フォーマット
Dcert
9303
無線ノード制御
パケット送受信部
9302
無線 I/F
9301

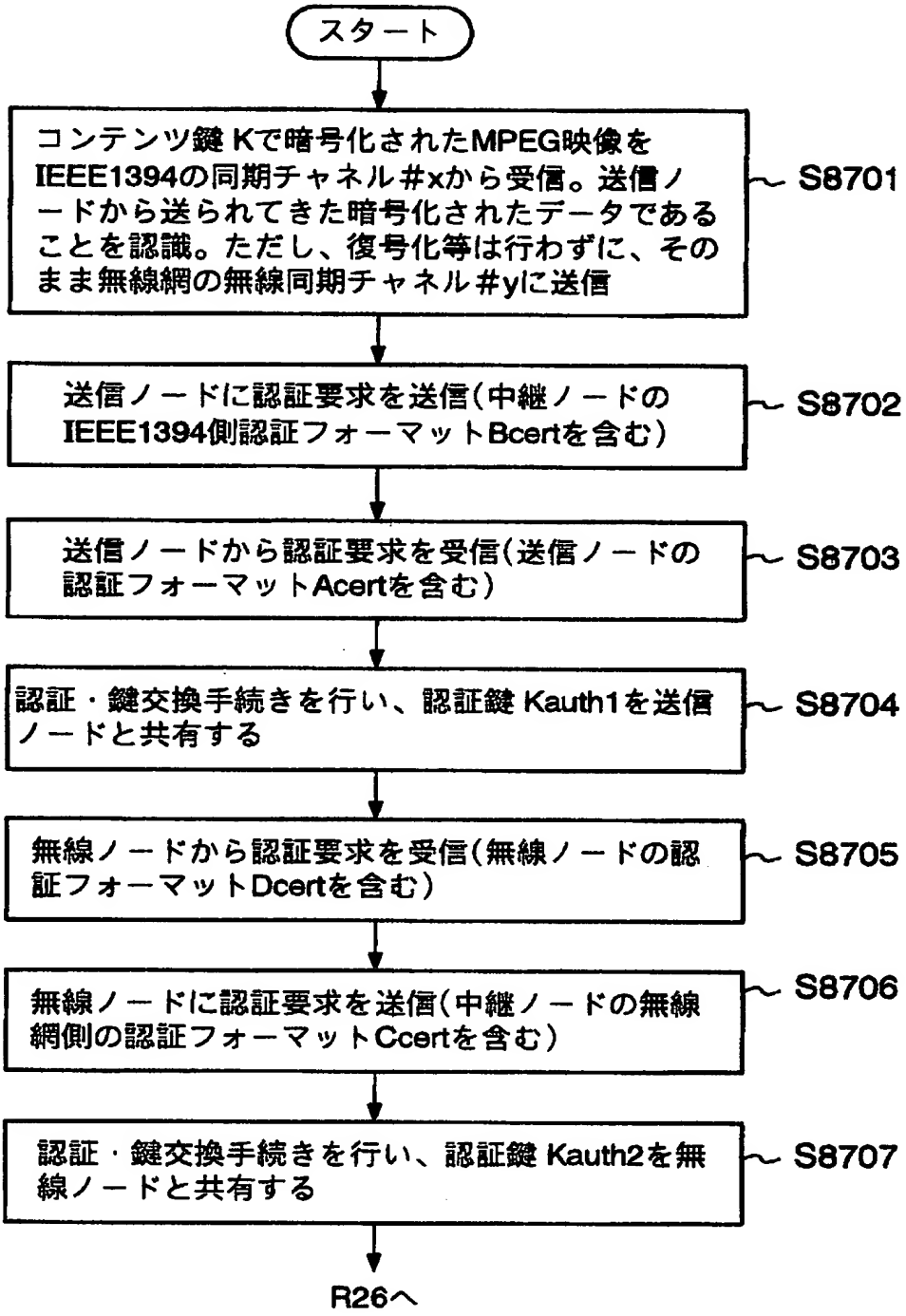
【図８１】


送信ノード 9101
中継ノード 9102
無線ノード 9103
[MPEG映像]k（#x経由）
S8501
認証要求
To:送信ノード、Bcert
S8502
認証要求
To:中継ノード、Acert
S8503
S8504
Kauth1
共有
認証・鍵交換手続き
S8505
Kauth1
共有
f（Kx、Kauth1）
S8506
Kx
シードNc転送
S8507
Nc
[MPEG映像]k（#x経由）
S8508
[MPEG映像]k（#y経由）
S8509
認証要求
To:中継ノード、Dcert
S8510
認証要求
To:無線ノード、Ccert
S8511
S8512
認証・鍵交換手続き
S8513
Kauth2
共有
Kauth2
共有
f（Kx、Kauth2）
S8514
Kx
シードNc転送
S8515
Nc
kの計算
S8516
[MPEG映像]k（#y経由）
S8517
暗号復号化、
デコード
S8518

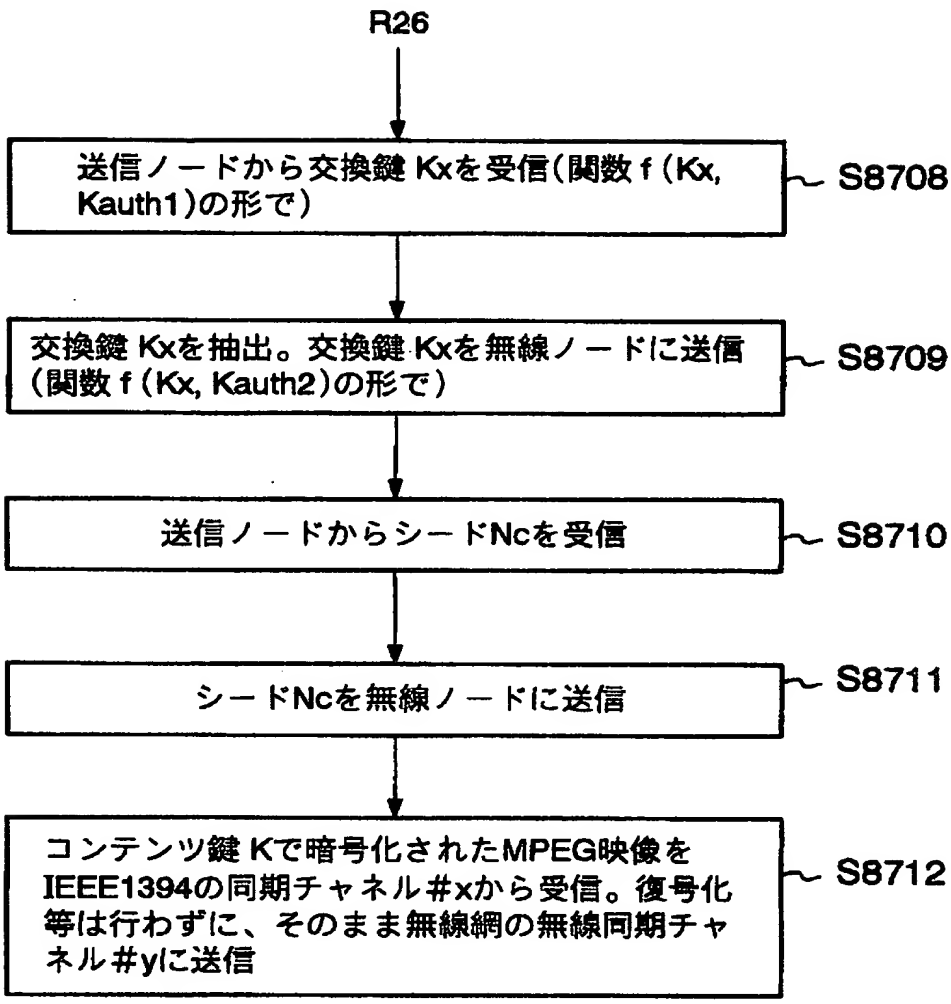
【図８２】


スタート
コンテンツ鍵Kで暗号化されたMPEG映像を同期チャネル#xに送出
S8601
中継ノードから認証要求を受信(中継ノードの認証フォーマットBcertを含む)
S8602
中継ノードに認証要求を送信(送信ノードの認証フォーマットAcertを含む)
S8603
認証・鍵交換手続きを行い、認証鍵Kauth1を中継ノードと共有する
S8604
交換鍵Kxを中継ノードに送信(関数f(Kx, Kauth1)の形で)
S8605
シードNcを中継ノードに送信
S8606
コンテンツ鍵Kで暗号化されたMPEG映像を同期チャネル#xに送出
S8607

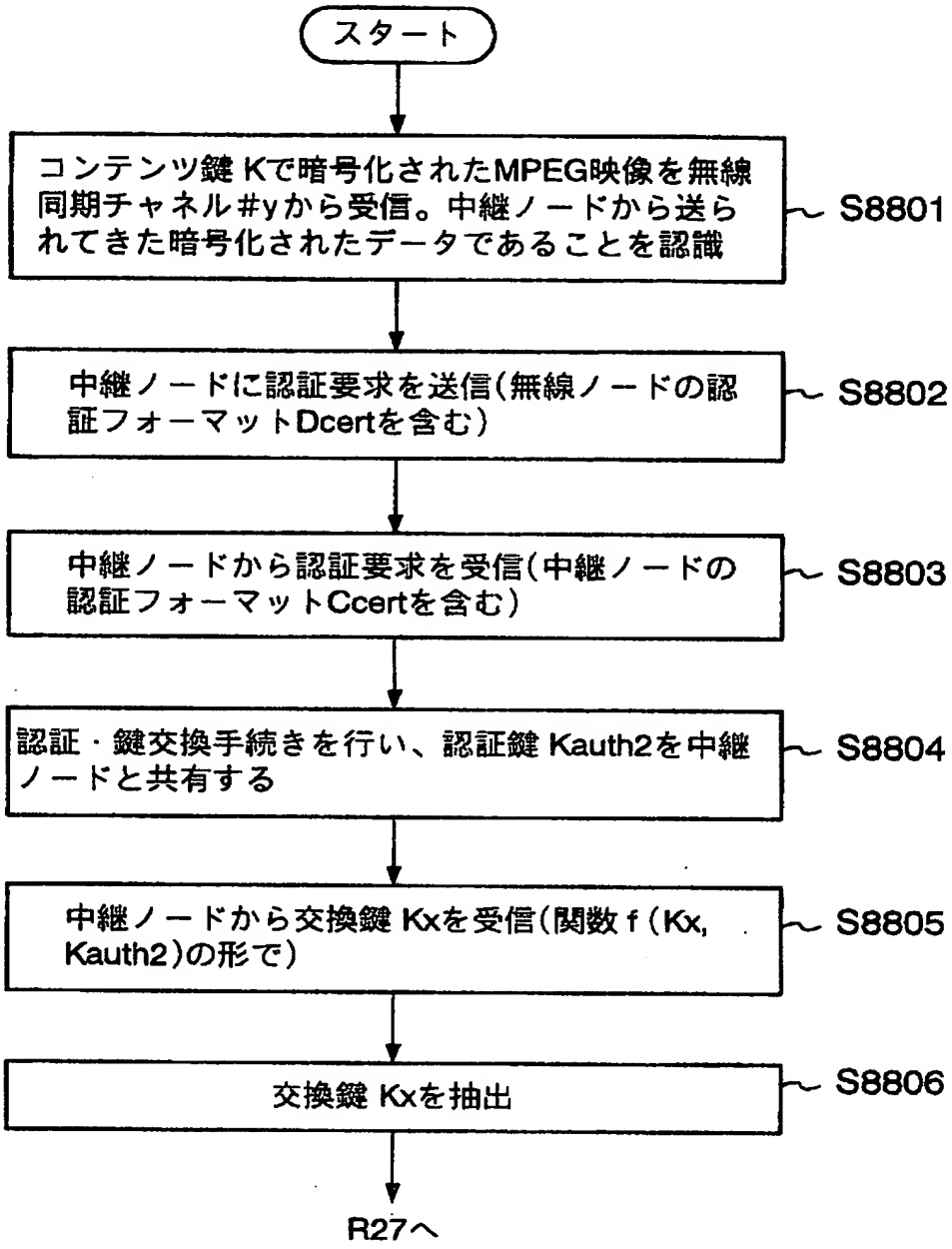
【図８３】


スタート
コンテンツ鍵Kで暗号化されたMPEG映像をIEEE1394の同期チャネル#xから受信。送信ノードから送られてきた暗号化されたデータであることを認識。ただし、復号化等は行わずに、そのまま無線網の無線同期チャネル#yに送信
S8701
送信ノードに認証要求を送信(中継ノードのIEEE1394側認証フォーマットBcertを含む)
S8702
送信ノードから認証要求を受信(送信ノードの認証フォーマットAcertを含む)
S8703
認証・鍵交換手続きを行い、認証鍵Kauth1を送信ノードと共有する
S8704
無線ノードから認証要求を受信(無線ノードの認証フォーマットDcertを含む)
S8705
無線ノードに認証要求を送信(中継ノードの無線網側の認証フォーマットCcertを含む)
S8706
認証・鍵交換手続きを行い、認証鍵Kauth2を無線ノードと共有する
S8707
R26へ

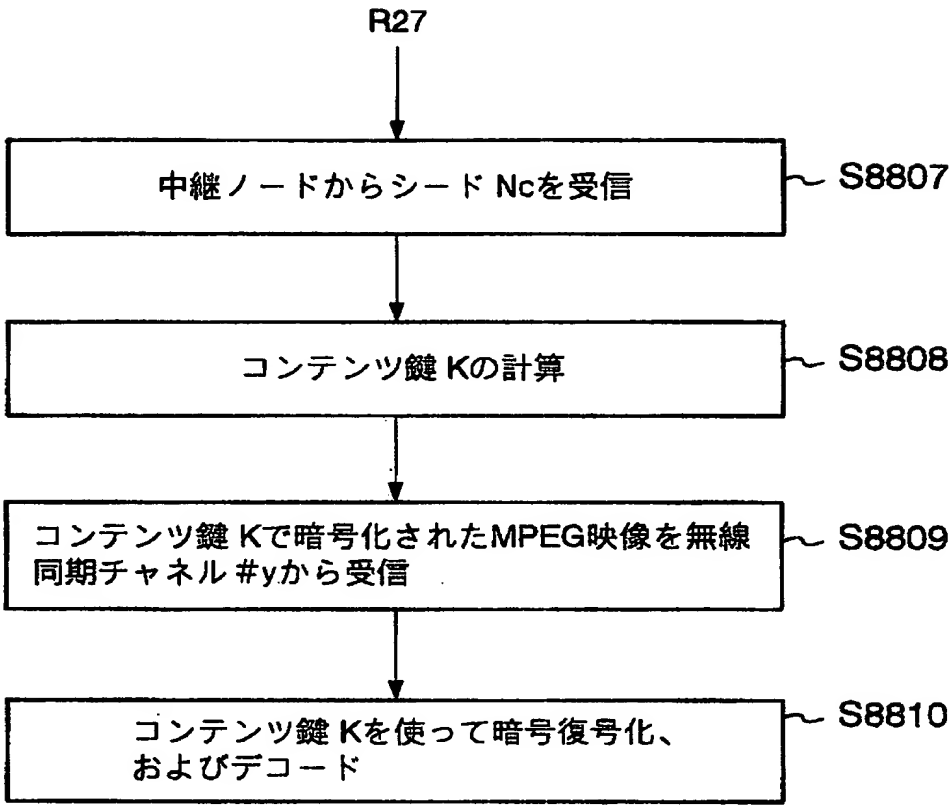
【図８４】


R26
送信ノードから交換鍵Kxを受信(関数f(Kx, Kauth1)の形で)
S8708
交換鍵Kxを抽出。交換鍵Kxを無線ノードに送信(関数f(Kx, Kauth2)の形で)
S8709
送信ノードからシードNcを受信
S8710
シードNcを無線ノードに送信
S8711
コンテンツ鍵Kで暗号化されたMPEG映像をIEEE1394の同期チャネル#xから受信。復号化等は行わずに、そのまま無線網の無線同期チャネル#yに送信
S8712

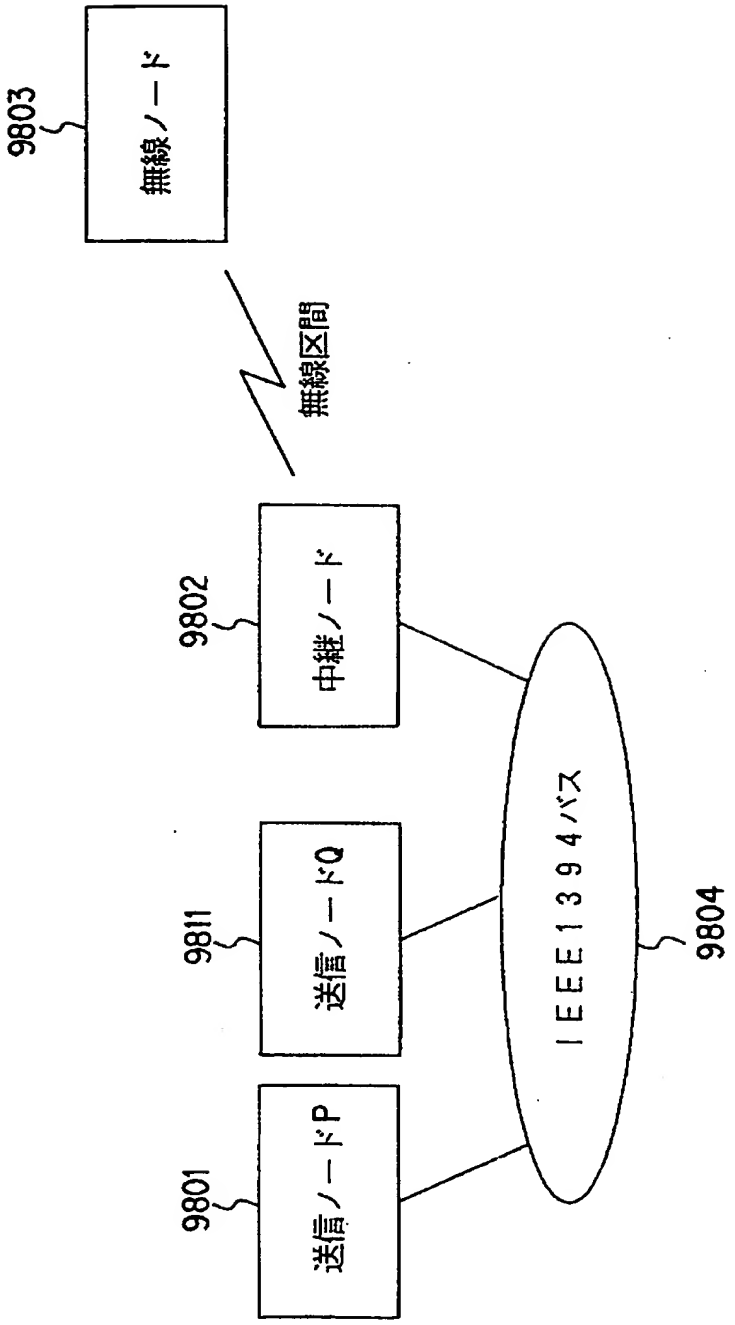
【図８５】


スタート
コンテンツ鍵 Kで暗号化されたMPEG映像を無線同期チャネル#yから受信。中継ノードから送られてきた暗号化されたデータであることを認識
S8801
中継ノードに認証要求を送信(無線ノードの認証フォーマットDcertを含む)
S8802
中継ノードから認証要求を受信(中継ノードの認証フォーマットCcertを含む)
S8803
認証・鍵交換手続きを行い、認証鍵 Kauth2を中継ノードと共有する
S8804
中継ノードから交換鍵 Kxを受信(関数 f (Kx, Kauth2)の形で)
S8805
交換鍵 Kxを抽出
S8806
R27へ

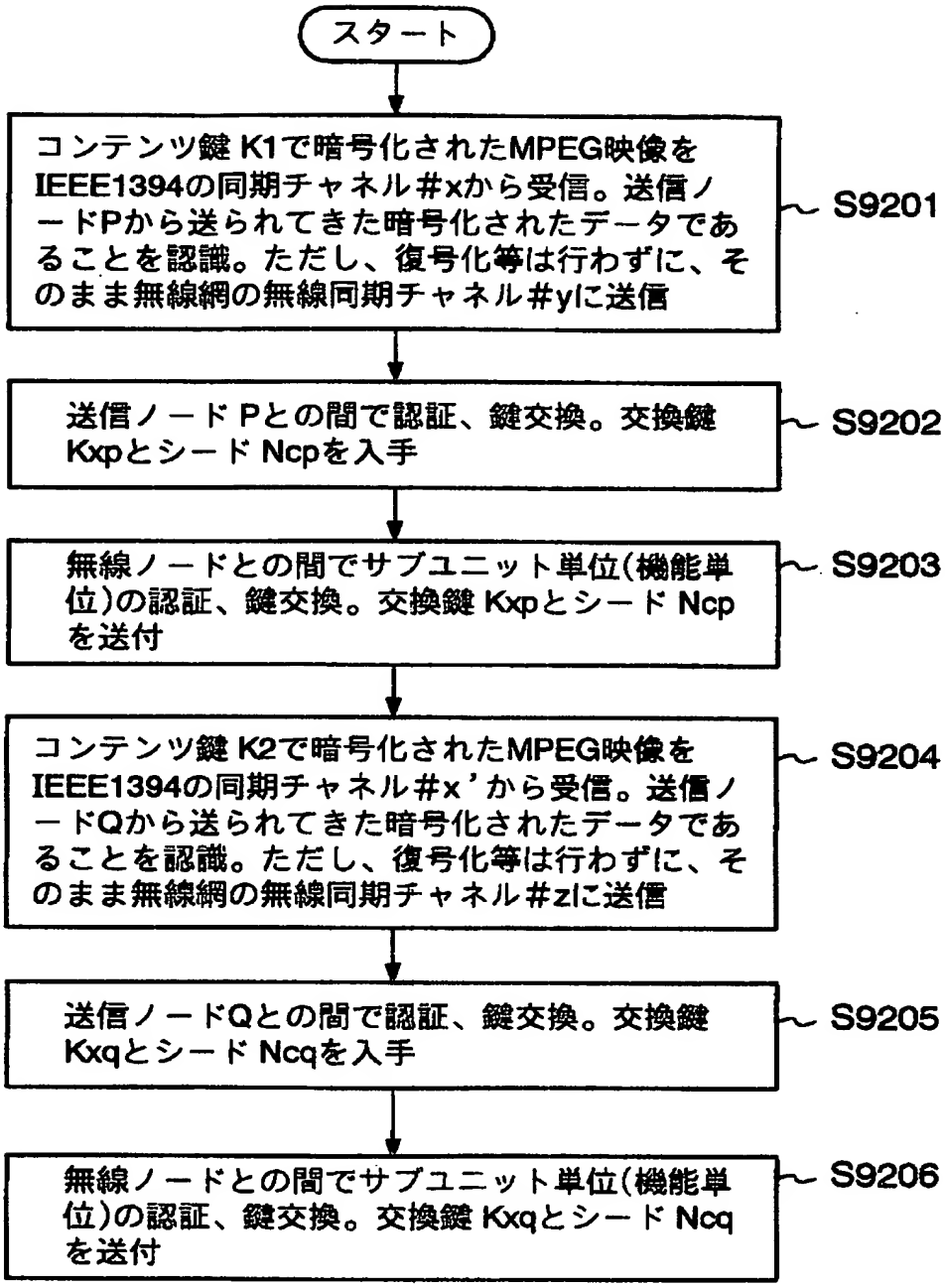
【図８６】


R27
中継ノードからシードNcを受信
S8807
コンテンツ鍵Kの計算
S8808
コンテンツ鍵Kで暗号化されたMPEG映像を無線同期チャネル#yから受信
S8809
コンテンツ鍵Kを使って暗号復号化、およびデコード
S8810

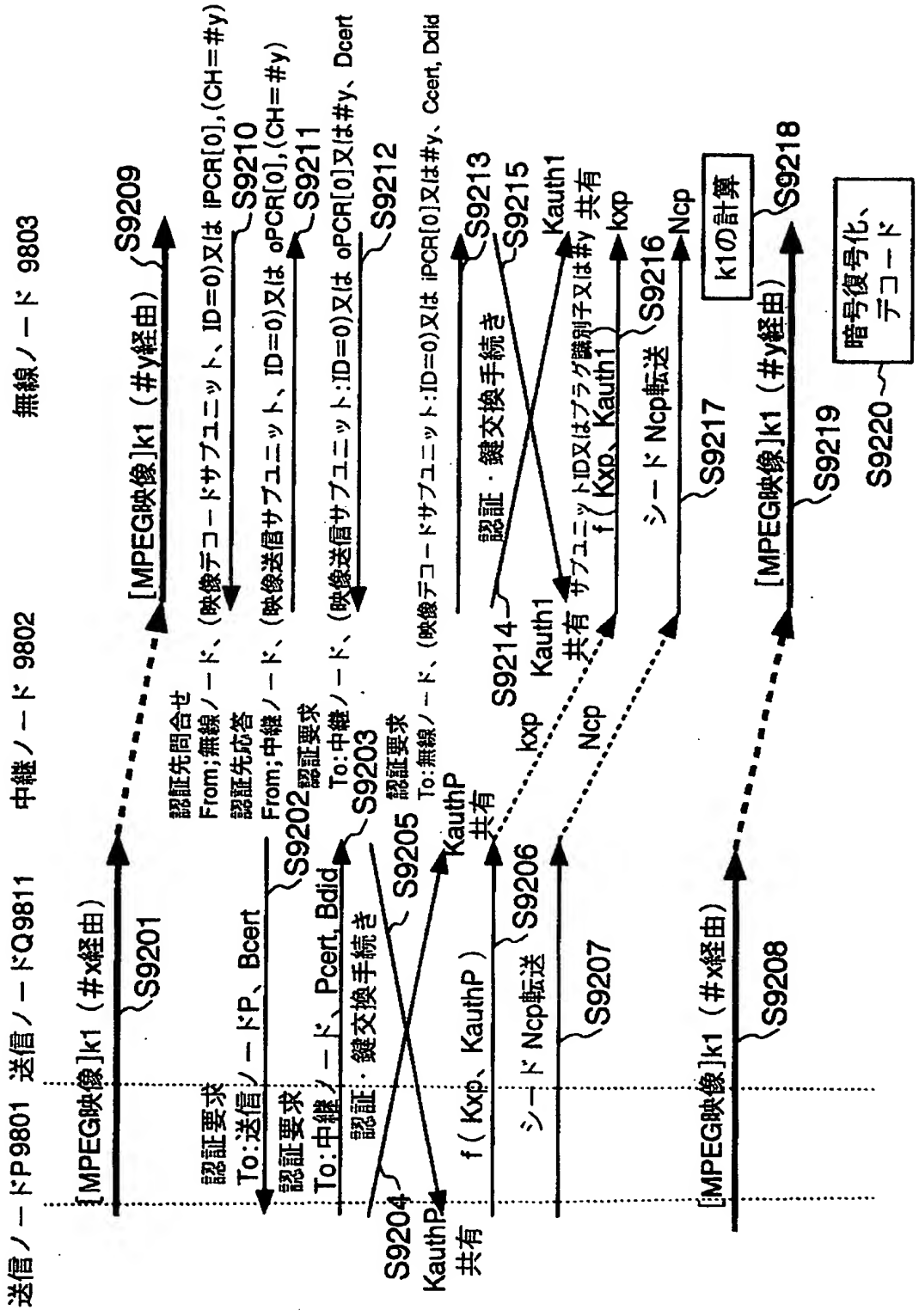
【図８７】


9803
無線ノード
無線区間
9802
中継ノード
9811
送信ノードQ
9801
送信ノードP
IEEE1394バス
9804

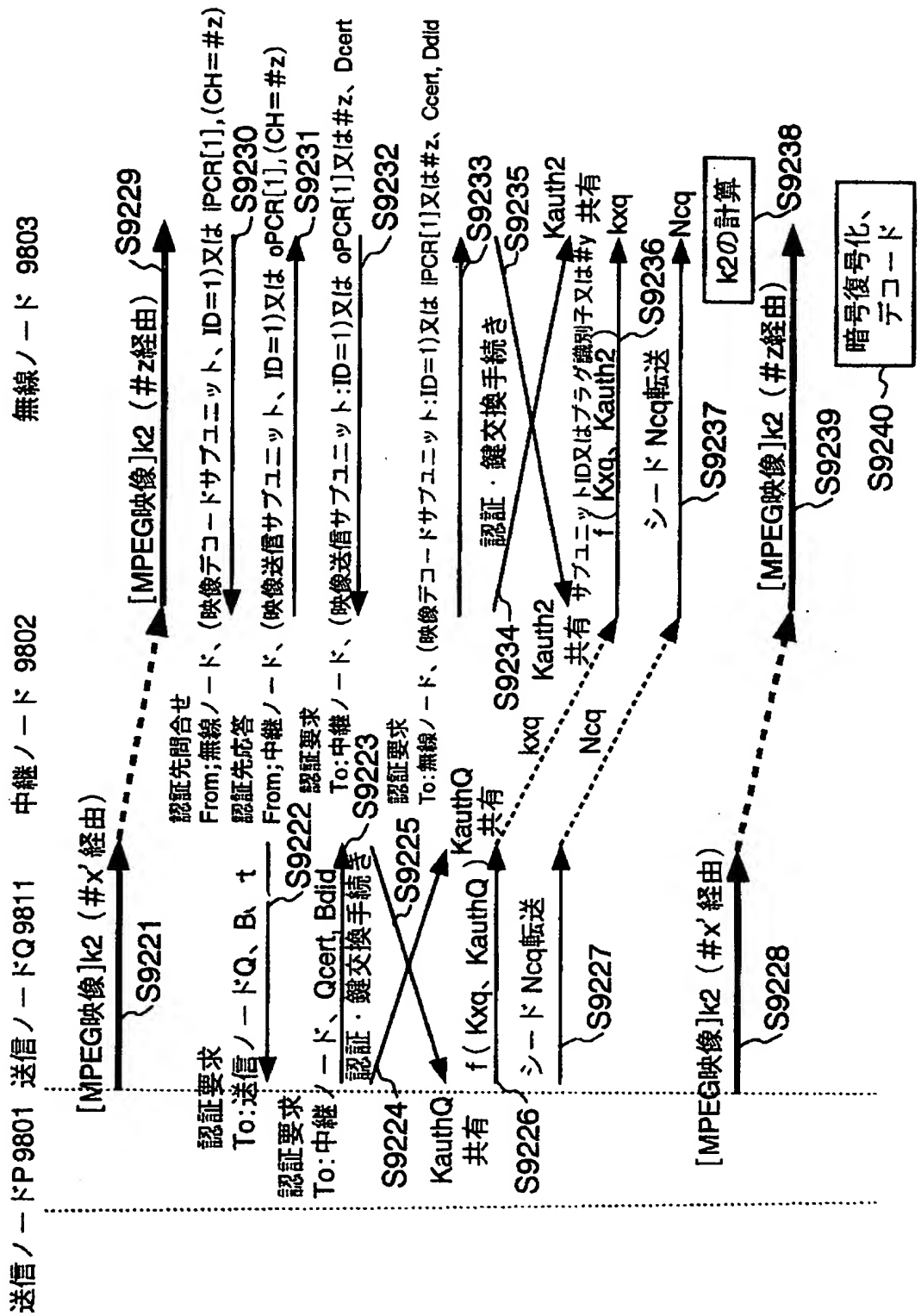
【図８８】


スタート
コンテンツ鍵 K1で暗号化されたMPEG映像をIEEE1394の同期チャネル#xから受信。送信ノードPから送られてきた暗号化されたデータであることを認識。ただし、復号化等は行わずに、そのまま無線網の無線同期チャネル#yに送信
S9201
送信ノード Pとの間で認証、鍵交換。交換鍵 Kxpとシード Ncpを入手
S9202
無線ノードとの間でサブユニット単位(機能単位)の認証、鍵交換。交換鍵 Kxpとシード Ncpを送付
S9203
コンテンツ鍵 K2で暗号化されたMPEG映像をIEEE1394の同期チャネル#x'から受信。送信ノードQから送られてきた暗号化されたデータであることを認識。ただし、復号化等は行わずに、そのまま無線網の無線同期チャネル#zに送信
S9204
送信ノードQとの間で認証、鍵交換。交換鍵 Kxqとシード Ncqを入手
S9205
無線ノードとの間でサブユニット単位(機能単位)の認証、鍵交換。交換鍵 Kxqとシード Ncqを送付
S9206

【図８９】


送信ノードP9801
送信ノードQ9811
中継ノード 9802
無線ノード 9803
[MPEG映像]k1（#x経由）
S9201
[MPEG映像]k1（#y経由）
S9209
認証先問合せ
From;無線ノード、(映像デコードサブユニット、ID=0)又は iPCR[0],(CH=#y)
S9210
認証先応答
To:送信ノードP、Bcert
From;中継ノード、(映像送信サブユニット、ID=0)又は oPCR[0],(CH=#y)
S9211
S9202
認証要求
To:中継ノード、Pcert, Bdid
S9203
認証要求
To:無線ノード、(映像デコードサブユニット:ID=0)又は iPCR[0]又は #y、Ccert, Ddid
S9212
S9204
認証・鍵交換手続き
KauthP
共有
S9205
KauthP
共有
f（Kxp、KauthP）
S9206
kxp
S9214
Kauth1
共有
S9213
認証・鍵交換手続き
S9215
Kauth1
サブユニットID又はプラグ識別子又は#y
f（Kxp、Kauth1）
共有
kxp
シードNcp転送
S9207
Ncp
S9216
シードNcp転送
Ncp
S9217
[MPEG映像]k1（#x経由）
S9208
[MPEG映像]k1（#y経由）
S9219
S9218
k1の計算
暗号復号化、デコード
S9220

【図９０】


送信ノードP 9801
送信ノードQ 9811
中継ノード 9802
無線ノード 9803
[MPEG映像]k2（#x'経由）
S9221
認証要求
To:送信ノードQ、Bid、t
S9222
認証先問合せ
From;無線ノード、(映像デコードサブユニット、ID=1)又は iPCR[1],(CH=#z)
S9230
認証先応答
From;中継ノード、(映像送信サブユニット、ID=1)又は oPCR[1],(CH=#z)
S9231
認証要求
To:中継ノード、Qcert, Bdid
S9223
認証要求
To:中継ノード、(映像送信サブユニット:ID=1)又は oPCR[1]又は#z、Dcert
S9232
認証・鍵交換手続き
S9224
認証要求
To:無線ノード、(映像デコードサブユニット:ID=1)又は iPCR[1]又は#z、Ccert, Ddid
S9233
KauthQ
共有
S9225
認証・鍵交換手続き
S9234
f（Kxq、KauthQ）
kxq
Kauth2
共有
S9235
Kauth2
サブユニットID又はブラグ識別子又は#y
f（Kxq、Kauth2）
共有
kxq
S9226
シード Ncq転送
S9227
Ncq
S9236
シード Ncq転送
S9237
Ncq
k2の計算
[MPEG映像]k2（#x'経由）
S9228
[MPEG映像]k2（#z経由）
S9238
S9239
暗号復号化、
デコード
S9240

【書類名】　　要約書

【要約】

【課題】　同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置を提供すること。

【解決手段】　第１のネットワーク１０４と第２のネットワークに接続され、第２のネットワーク上の装置１０３を自中継装置１０２上のものとして第１のネットワーク１０４側に開示する機能と、第１のネットワーク１０４上の装置１０１から装置１０３宛の制御コマンドを受信した場合、これに対応する制御コマンドを装置１０３へ送信する機能と、装置１０１から装置１０３宛のコンテンツ保護情報を受信した場合、これに変更を加えずに装置１０３へ送信する機能と、装置１０１から装置１０３宛に先のコンテンツ保護情報から得られるコンテンツ鍵で保護されたコンテンツを受信した場合、これに変更を加えずに装置１０３へ送信する機能とを有する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　　神奈川県川崎市幸区堀川町７２番地
氏　名　　株式会社東芝